Руководво по настройке

Ethernet-коммутаторы агрегации

Настройка IP-адреса и приложений QSW-6300

Оглавление

1. НАСТРОЙКА IP-АДРЕСОВ И СЕРВИСОВ 20
1.1. Обзор 20
1.1.1. Протоколы и стандарты 20
1.2. Применение 20
1.2.1. Настройка IP-адреса для связи 20
1.2.1.1. Сценарий 20
1.2.1.2. Настройка 20
1.3. Ключевые особенности 21
1.3.1. Базовые концепции 21
1.3.1.1. IP-адрес 21
1.3.1.2. Маска подсети 23
1.3.1.3. Широковещательный (Broadcast) пакет 23
1.3.1.4. Пакет ICMP 23
1.3.1.5. TTL 23
1.3.2. Ключевые особенности 24
1.3.3. IP-адрес 24
1.3.3.1. Настройка IP-адреса для интерфейса 24
1.3.3.2. Настройка нескольких IP-адресов для интерфейса 24
1.3.3.3. Связанная конфигурация 25
1.3.4. Обработка широковещательных (Broadcast) пакетов 26
1.3.4.1. Принцип работы 26
1.3.4.2. Связанная конфигурация 26
1.3.5. Отправка пакетов ICMP 27
1.3.5.1. Принцип работы 27
1.3.5.2. Связанная конфигурация 27
1.3.6. Ограничение скорости передачи пакетов ошибок ICMP 28
1.3.6.1. Принцип работы 28
1.3.6.2. Связанная конфигурация 28
1.3.7. IP MTU 28
1.3.7.1. Принцип работы 28
1.3.7.2. Связанная конфигурация 28
1.3.8. IP TTL 28
1.3.8.1. Принцип работы 28
1.3.8.2. Связанная конфигурация 29
1.3.9. Маршрут источника IP (IP Source routing) 29
1.3.9.1. Принцип работы 29

1.3.9.2. Связанная конфигурация 29
1.4. Настройка 29
1.4.1. Настройка IP-адресов интерфейса 31
1.4.1.1. Результат конфигурации 31
1.4.1.2. Этапы конфигурации 31
1.4.1.3. Проверка конфигурации 31
1.4.1.4. Связанные команды 31
1.4.1.5. Пример конфигурации 33
1.4.2. Настройка передачи широковещательной рассылки 34
1.4.2.1. Результат конфигурации 34
1.4.2.2. Этапы конфигурации 34
1.4.2.3. Проверка конфигурации 34
1.4.2.4. Связанные команды 34
1.4.2.5. Пример конфигурации 35
1.4.3. Настройка пересылки ICMP 35
1.4.3.1. Результат конфигурации 35
1.4.3.2. Этапы конфигурации 35
1.4.3.3. Проверка конфигурации 36
1.4.3.4. Связанные команды 36
1.4.3.5. Пример конфигурации 36
1.4.4. Настройка скорости передачи пакетов ошибок ICMP 37
1.4.4.1. Результат конфигурации 37
1.4.4.2. Этапы конфигурации 37
1.4.4.3. Проверка конфигурации 37
1.4.4.4. Связанные команды 37
1.4.4.5. Пример конфигурации 39
1.4.5. Установка значения IP MTU 39
1.4.5.1. Результат конфигурации 39
1.4.5.2. Этапы конфигурации 39
1.4.5.3. Проверка конфигурации 39
1.4.5.4. Связанные команды 40
1.4.5.5. Пример конфигурации 40
1.4.6. Установка значения IP TTL 40
1.4.6.1. Результат конфигурации 40
1.4.6.2. Этапы конфигурации 40
1.4.6.3. Проверка конфигурации 40
1.4.6.4. Связанные команды 41
1.4.6.5. Пример конфигурации 41

1.4.7. Настройка IP Source routing 41
1.4.7.1. Результат конфигурации 41
1.4.7.2. Этапы конфигурации 41
1.4.7.3. Проверка конфигурации 41
1.4.7.4. Связанные команды 41
1.4.7.5. Пример конфигурации 42
1.5. Контроль состояния 42
1.5.1. Отображение 42
2. НАСТРОЙКА ARP 43
2.1. Обзор 43
2.1.1. Протоколы и стандарты 43
2.2. Применение 43
2.2.1. ARP в локальной сети 43
2.2.1.1. Сценарий 43
2.2.1.2. Описание 44
2.2.2. Прозрачная передача на основе протокола Proxy ARP 44
2.2.2.1. Сценарий 44
2.2.2.2. Описание 44
2.3. Ключевые особенности 45
2.3.1. Обзор 45
2.3.2. Статический ARP 45
2.3.2.1. Принцип работы 45
2.3.2.2. Связанная конфигурация 46
2.3.3. Атрибуты ARP 46
2.3.3.1. Принцип работы 46
2.3.3.2. Связанная конфигурация 46
2.3.4. Trusted ARP 47
2.3.4.1. Принцип работы 47
2.3.4.2. Связанная конфигурация 47
2.3.5. Gratuitous ARP 48
2.3.5.1. Принцип работы 48
2.3.5.2. Связанная конфигурация 48
2.3.6. Proxy ARP 48
2.3.6.1. Принцип работы 48
2.3.6.2. Связанная конфигурация 48
2.3.7. Local Proxy ARP 48
2.3.7.1. Принцип работы 48

2.3.7.2. Связанная конфигурация 49
2.3.8. Определение надежности ARP 49
2.3.8.1. Принцип работы 49
2.3.8.2. Связанная конфигурация 49
2.3.9. IP Guard на основе ARP 49
2.3.9.1. Принцип работы 49
2.3.9.2. Связанная конфигурация 50
2.3.10. Преобразование запросов ARP в запросы аутентификации VLAN 50
2.3.10.1. Принцип работы 50
2.3.10.2. Связанная конфигурация 50
2.4. Настройка 50
2.4.1. Включение статического ARP 52
2.4.1.1. Результат конфигурации 52
2.4.1.2. Примечания 52
2.4.1.3. Этапы конфигурации 52
2.4.1.4. Проверка конфигурации 52
2.4.1.5. Связанные команды 53
2.4.1.6. Пример конфигурации 53
2.4.1.7. Типичные ошибки 53
2.4.2. Настройка атрибутов ARP 54
2.4.2.1. Результат конфигурации 54
2.4.2.2. Этапы конфигурации 54
2.4.2.3. Проверка конфигурации 54
2.4.2.4. Связанные команды 54
2.4.2.5. Пример конфигурации 55
2.4.3. Включение trusted ARP 56
2.4.3.1. Результат конфигурации 56
2.4.3.2. Этапы конфигурации 56
2.4.3.3. Проверка конфигурации 56
2.4.3.4. Связанные команды 57
2.4.3.5. Пример конфигурации 59
2.4.3.6. Типичные ошибки 59
2.4.4. Включение Gratuitous ARP 59
2.4.4.1. Результат конфигурации 59
2.4.4.2. Этапы конфигурации 59
2.4.4.3. Проверка конфигурации 60
2.4.4.4. Связанные команды 60
2.4.4.5. Пример конфигурации 60

2.4.5. Включение защиты IP-адресов на основе ARP 61
2.4.5.1. Результат конфигурации 61
2.4.5.2. Этапы конфигурации 61
2.4.5.3. Проверка конфигурации 61
2.4.5.4. Связанные команды 61
2.4.5.5. Пример конфигурации 62
2.4.6. Преобразование запросов ARP в запросы аутентификации VLAN 62
2.4.6.1. Результат конфигурации 62
2.4.6.2. Примечания 62
2.4.6.3. Этапы конфигурации 62
2.4.6.4. Проверка конфигурации 62
2.4.6.5. Связанные команды 62
2.4.6.6. Пример конфигурации 63
2.5. Контроль состояния 63
2.5.1. Очистка 63
2.5.2. Отображение 64
2.5.3. Отладка 64
3. НАСТРОЙКА IPV6 65
3.1. Обзор 65
3.1.1. Основные функции 65
3.1.1.1. Протоколы и стандарты 66
3.2. Применение 66
3.2.1. Связь на основе адресов IPv6 66
3.2.1.1. Сценарий 66
3.2.1.2. Описание 67
3.3. Ключевые особенности 67
3.3.1. Обзор 67
3.3.2. Формат адреса IPv6 68
3.3.2.1. Связанная конфигурация 69
3.3.3. Тип адреса IPv6 69
3.3.3.1. Связанная конфигурация 73
3.3.4. Формат заголовка пакета IPv6 73
3.3.5. IPv6 PMTUD (Path MTU Discovery) 74
3.3.5.1. Связанная конфигурация 75
3.3.6. Обнаружение соседей IPv6 75
3.3.6.1. Связанная конфигурация 78
3.3.7. Маршрут источника IPv6 (IPv6 Source Routing) 79

3.3.7.1. Принцип работы 79
3.3.7.2. Связанная конфигурация 82
3.3.8. Ограничение скорости отправки сообщений об ошибках ICMPv6 82
3.3.8.1. Принцип работы 82
3.3.8.2. Связанная конфигурация 83
3.3.9. Ограничение перехода IPv6(IPv6 Hop Limit) 83
3.3.9.1. Принцип работы 83
3.3.9.2. Связанная конфигурация 83
3.3.10. Преобразование из отправки пакетов NS в сети аутентификации VLAN 83
3.3.10.1. Принцип работы 83
3.3.10.2. Связанная конфигурация 83
3.3.11. Шлюз по умолчанию в интерфейсе управления 84
3.3.11.1. Принцип работы 84
3.3.11.2. Связанная конфигурация 84
3.4. Настройка 84
3.4.1. Настройка IPv6-адреса 86
3.4.1.1. Результат конфигурации 86
3.4.1.2. Этапы конфигурации 86
3.4.1.3. Проверка конфигурации 86
3.4.1.4. Связанные команды 86
3.4.1.5. Пример конфигурации 88
3.4.2. Настройка IPv6 NDP 89
3.4.2.1. Результат конфигурации 89
3.4.2.2. Примечания 89
3.4.2.3. Этапы конфигурации 89
3.4.2.4. Проверка конфигурации 90
3.4.2.5. Связанные команды 90
3.4.2.6. Пример конфигурации 94
3.4.3. Настройка MTU IPv6 на интерфейсе 98
3.4.3.1. Результат конфигурации 98
3.4.3.2. Примечания 98
3.4.3.3. Этапы конфигурации 98
3.4.3.4. Проверка конфигурации 98
3.4.3.5. Связанные команды 98
3.4.3.6. Пример конфигурации 99
3.4.4. Включение маршрута источника IPv6 (IPv6 Source Routing) 99
3.4.4.1. Результат конфигурации 99
3.4.4.2. Этапы конфигурации 99

3.4.4.3. Проверка конфигурации 100
3.4.4.4. Связанные команды 100
3.4.4.5. Пример конфигурации 100
3.4.5. Настройка скорости отправки сообщений об ошибках ICMPv6 100
3.4.5.1. Результат конфигурации 100
3.4.5.2. Этапы конфигурации 100
3.4.5.3. Проверка конфигурации 101
3.4.5.4. Связанные команды 101
3.4.5.5. Пример конфигурации 102
3.4.6. Настройка значения IPv6 Hop Limit 103
3.4.6.1. Результат конфигурации 103
3.4.6.2. Этапы конфигурации 103
3.4.6.3. Проверка конфигурации 103
3.4.6.4. Связанные команды 103
3.4.6.5. Пример конфигурации 103
3.4.7. Включение/выключение функции отказа отправки пакетов NS в сети VLAN аутентификации 104
3.4.7.1. Результат конфигурации 104
3.4.7.2. Примечания 104
3.4.7.3. Этапы конфигурации 104
3.4.7.4. Проверка конфигурации 104
3.4.7.5. Связанные команды 104
3.4.7.6. Пример конфигурации 104
3.4.8. Настройка шлюза по умолчанию в интерфейсе управления 105
3.4.8.1. Результат конфигурации 105
3.4.8.2. Примечания 105
3.4.8.3. Этапы конфигурации 105
3.4.8.4. Проверка конфигурации 105
3.4.8.5. Связанные команды 105
3.4.8.6. Пример конфигурации 105
3.5. Контроль состояния 106
3.5.1. Очистка 106
3.5.2. Отображение 106
3.5.3. Отладка 106
4. НАСТРОЙКА DHCP 107
4.1. Обзор 107
4.1.1. Протоколы и стандарты 107
4.2. Применение 107

4.2.1. Предоставление службы DHCP в локальной сети 107
4.2.1.1. Сценарий 107
4.2.1.2. Описание 108
4.2.2. Включение клиента DHCP 108
4.2.2.1. Сценарий 108
4.2.2.2. Описание 108
4.2.3. Применение правила AM на сервере DHCP 109
4.2.3.1. Сценарий 109
4.2.3.2. Описание 109
4.2.4. Настройка DHCP Relay в проводной сети 110
4.2.4.1. Сценарий 110
4.2.4.2. Описание 110
4.2.5. Применение правила AM на DHCP Relay 110
4.2.5.1. Сценарий 110
4.2.5.2. Описание 111
4.3. Ключевые особенности 112
4.3.1. Базовые концепции 112
4.3.2. Обзор 112
4.3.3. Сервер DHCP 113
4.3.3.1. Принцип работы 113
4.3.3.2. Связанная конфигурация 114
4.3.4. Агент DHCP Relay 115
4.3.4.1. Принцип работы 115
4.3.4.2. Связанная конфигурация 117
4.3.5. Клиент DHCP 118
4.3.5.1. Принцип работы 118
4.3.5.2. Связанная конфигурация 118
4.3.6. Правила AM 118
4.3.6.1. Принцип работы 118
4.3.6.2. Связанная конфигурация 119
4.4. Настройка 119
4.4.1. Настройка сервера DHCP 119
4.4.2. Настройка DHCP-ретрансляции 121
4.4.3. Настройка клиента DHCP 122
4.4.4. Настройка динамического IP-адреса 122
4.4.4.1. Результат конфигурации 122
4.4.4.2. Примечания 122
4.4.4.3. Этапы конфигурации 122

4.4.4.4. Проверка конфигурации 124
4.4.4.5. Связанные команды 124
4.4.4.6. Пример конфигурации 129
4.4.5. Настройка статического IP-адреса 129
4.4.5.1. Результат конфигурации 129
4.4.5.2. Этапы конфигурации 129
4.4.5.3. Проверка конфигурации 130
4.4.5.4. Связанные команды 130
4.4.5.5. Пример конфигурации 131
4.4.6. Настройка правила AM для сервера DHCP 132
4.4.6.1. Результат конфигурации 132
4.4.6.2. Примечания 132
4.4.6.3. Этапы конфигурации 132
4.4.6.4. Проверка конфигурации 132
4.4.6.5. Связанные команды 133
4.4.6.6. Пример конфигурации 134
4.4.7. Настройка глобальных свойств DHCP-сервера 134
4.4.7.1. Результат конфигурации 134
4.4.7.2. Примечания 134
4.4.7.3. Этапы конфигурации 134
4.4.7.4. Проверка конфигурации 135
4.4.7.5. Связанные команды 135
4.4.7.6. Пример конфигурации 137
4.4.8. Настройка основных функций DHCP Relay 138
4.4.8.1. Результат конфигурации 138
4.4.8.2. Примечания 138
4.4.8.3. Этапы конфигурации 138
4.4.8.4. Проверка конфигурации 138
4.4.8.5. Связанные команды 138
4.4.8.6. Пример конфигурации 139
4.4.8.7. Типичные ошибки 140
4.4.9. Настройка DHCP Relay опции 82 140
4.4.9.1. Результат конфигурации 140
4.4.9.2. Примечания 140
4.4.9.3. Этапы конфигурации 140
4.4.9.4. Проверка конфигурации 141
4.4.9.5. Связанные команды 141
4.4.9.6. Пример конфигурации 141

4.4.9.7. Типичные ошибки 141
4.4.10. Настройка проверки Server ID для DHCP Relay 141
4.4.10.1. Результат конфигурации 141
4.4.10.2. Примечания 141
4.4.10.3. Этапы конфигурации 142
4.4.10.4. Проверка конфигурации 142
4.4.10.5. Связанные команды 142
4.4.10.6. Пример конфигурации 142
4.4.10.7. Типичные ошибки 142
4.4.11. Настройка подавления DHCP Relay 142
4.4.11.1. Результат конфигурации 142
4.4.11.2. Примечания 143
4.4.11.3. Этапы конфигурации 143
4.4.11.4. Проверка конфигурации 143
4.4.11.5. Связанные команды 143
4.4.11.6. Пример конфигурации 143
4.4.11.7. Типичные ошибки 143
4.4.12. Настройка клиента DHCP 144
4.4.12.1. Результат конфигурации 144
4.4.12.2. Примечания 144
4.4.12.3. Этапы конфигурации 144
4.4.12.4. Проверка конфигурации 144
4.4.12.5. Связанные команды 144
4.4.12.6. Пример конфигурации 144
4.5. Контроль состояния 145
4.5.1. Очистка 145
4.5.2. Отображение 145
4.5.3. Отладка 146
5. НАСТРОЙКА DHCPV6 147
5.1. Обзор 147
5.1.1. Протоколы и стандарты 148
5.2. Применение 148
5.2.1. Запрос/назначение адресов и параметров конфигурации 148
5.2.1.1. Сценарий 148
5.2.1.2. Описание 149
5.2.2. Запрос/выделение префикса 149
5.2.2.1. Сценарий 149

5.2.2.2. Описание 150
5.2.3. Агент Relay 150
5.2.3.1. Сценарий 150
5.2.3.2. Описание 150
5.3. Ключевые особенности 150
5.3.1. Базовые концепции 150
5.3.2. Обзор 152
5.3.3. Запрос/выделение адресов 152
5.3.3.1. Принцип работы 152
5.3.3.2. Связанная конфигурация 156
5.3.4. Запрос/выделение префикса 156
5.3.4.1. Принцип работы 156
5.3.4.2. Связанная конфигурация 157
5.3.5. Служба без сохранения состояния 157
5.3.5.1. Принцип работы 157
5.3.5.2. Связанная конфигурация 157
5.3.6. DHCPv6 Relay 158
5.3.6.1. Принцип работы 158
5.4. Настройка 159
5.4.1. Настройка сервера DHCPv6 160
5.4.1.1. Результат конфигурации 160
5.4.1.2. Примечания 160
5.4.1.3. Этапы конфигурации 160
5.4.1.4. Проверка конфигурации 161
5.4.1.5. Связанные команды 161
5.4.1.6. Пример конфигурации 166
5.4.1.7. Типичные ошибки 167
5.4.2. Настройка DHCPv6 Relay 167
5.4.2.1. Результат конфигурации 167
5.4.2.2. Примечания 167
5.4.2.3. Этапы конфигурации 167
5.4.2.4. Проверка конфигурации 167
5.4.2.5. Связанные команды 168
5.4.2.6. Пример конфигурации 168
5.4.2.7. Типичные ошибки 169
5.5. Контроль состояния 169
5.5.1. Очистка 169
5.5.2. Отображение 169

5.5.2.1. Отладка 170
6. НАСТРОЙКА DNS 171
6.1. Обзор 171
6.1.1. Протоколы и стандарты 171
6.2. Применение 171
6.2.1. Статическое разрешение доменного имени 171
6.2.1.1. Сценарий 171
6.2.1.2. Описание 171
6.2.2. Динамическое разрешение доменного имени 171
6.2.2.1. Сценарий 171
6.2.3. Развертывания 172
6.3. Ключевые особенности 172
6.3.1. Базовые концепции 172
6.3.2. Ключевые особенности 172
6.3.3. Разрешение имени домена 172
6.3.3.1. Принцип работы 172
6.3.3.2. Связанная конфигурация 173
6.4. Настройка 173
6.4.1. Настройка статического разрешения доменного имени 174
6.4.1.1. Результат конфигурации 174
6.4.1.2. Этапы конфигурации 174
6.4.1.3. Проверка конфигурации 174
6.4.1.4. Связанные команды 174
6.4.1.5. Пример конфигурации 174
6.4.2. Настройка динамического разрешения доменного имени 175
6.4.2.1. Результат конфигурации 175
6.4.2.2. Этапы конфигурации 175
6.4.2.3. Проверка конфигурации 175
6.4.2.4. Связанные команды 175
6.4.2.5. Пример конфигурации 176
6.5. Контроль состояния 176
6.5.1. Очистка 176
6.5.2. Отображение 177
6.5.3. Отладка 177
7. НАСТРОЙКА СЕРВЕРА FTP 178
7.1. Обзор 178
7.1.1. Протоколы и стандарты 178

7.2. Применение 178
7.2.1. Предоставление службы FTP в локальной сети 178
7.2.1.1. Сценарий 178
7.2.1.2. Описание 178
7.3. Ключевые особенности 179
7.3.1. Базовые концепции 179
7.3.2. Обзор 181
7.3.3. Включение функции FTP-сервера 181
7.3.3.1. Принцип работы 181
7.3.3.2. Связанная конфигурация 181
7.4. Настройка 182
7.4.1. Настройка основных функций 182
7.4.1.1. Результат конфигурации 182
7.4.1.2. Примечания 182
7.4.1.3. Этапы конфигурации 182
7.4.1.4. Проверка конфигурации 183
7.4.1.5. Связанные команды 183
7.4.1.6. Пример конфигурации 186
7.4.1.7. Типичные ошибки 187
7.5. Контроль состояния 187
7.5.1. Отображение 187
7.5.2. Отладка 187
8. НАСТРОЙКА КЛИЕНТА FTP 188
8.1. Обзор 188
8.1.1. Протоколы и стандарты 188
8.2. Применение 188
8.2.1. Загрузка локального файла на удаленный сервер 188
8.2.1.1. Сценарий 188
8.2.1.2. Описание 189
8.2.2. Загрузка файла с удаленного сервера на локальное устройство 189
8.2.2.1. Сценарий 189
8.2.2.2. Описание 189
8.3. Ключевые особенности 189
8.3.1. Базовые концепции 189
8.3.2. Обзор 190
8.3.3. Загрузка файлов FTP 190
8.3.4. Скачивание файлов FTP 190

8.3.5. Режим подключения FTP 190
8.3.6. Режим передачи по FTP 192
8.3.7. Указание IP-адреса интерфейса источника для передачи по FTP 192
8.4. Настройка 193
8.4.1. Настройка основных функций 193
8.4.1.1. Результат конфигурации 193
8.4.1.2. Примечания 193
8.4.1.3. Этапы конфигурации 193
8.4.1.4. Проверка конфигурации 194
8.4.1.5. Связанные команды 194
8.4.1.6. Пример конфигурации 195
8.4.1.7. Типичные ошибки 195
8.4.2. Настройка дополнительных функций 196
8.4.2.1. Результат конфигурации 196
8.4.2.2. Примечания 196
8.4.2.3. Этапы конфигурации 196
8.4.2.4. Проверка конфигурации 196
8.4.2.5. Связанные команды 196
8.4.2.6. Пример конфигурации 198
8.4.2.7. Типичные ошибки 198
8.5. Контроль состояния 198
8.5.1. Отображение 198
8.5.2. Отладка 199
9. НАСТРОЙКА ТУННЕЛЬНОГО ИНТЕРФЕЙСА 200
9.1. Обзор 200
9.1.1. Протоколы и стандарты 200
9.2. Применение 201
9.2.1. Доступ к сайтам IPv6 в сети кампуса 201
9.2.1.1. Сценарий 201
9.2.1.2. Описание 202
9.3. Настройка 202
9.3.1. Настройка туннельного интерфейса 203
9.3.1.1. Результат конфигурации 203
9.3.1.2. Этапы конфигурации 203
9.3.1.3. Проверка конфигурации 203
9.3.1.4. Связанные команды 203
9.3.1.5. Пример конфигурации 204

9.3.1.6. Типичные ошибки 204
9.3.2. Настройка режима туннеля 204
9.3.2.1. Результат конфигурации 204
9.3.2.2. Этапы конфигурации 204
9.3.2.3. Проверка конфигурации 205
9.3.2.4. Связанные команды 205
9.3.2.5. Пример конфигурации 206
9.3.2.6. Типичные ошибки 206
9.3.3. Настройка локального адреса 206
9.3.3.1. Результат конфигурации 206
9.3.3.2. Примечания 206
9.3.3.3. Этапы конфигурации 206
9.3.3.4. Проверка конфигурации 207
9.3.3.5. Связанные команды 207
9.3.3.6. Пример конфигурации 207
9.3.4. Настройка адреса одноранговой сети 208
9.3.4.1. Результат конфигурации 208
9.3.4.2. Примечания 208
9.3.4.3. Этапы конфигурации 208
9.3.4.4. Проверка конфигурации 208
9.3.4.5. Связанные команды 208
9.3.4.6. Пример конфигурации 208
9.3.4.7. Типичные ошибки 209
9.3.5. Настройка TOS туннеля 209
9.3.5.1. Результат конфигурации 209
9.3.5.2. Примечания 209
9.3.5.3. Этапы конфигурации 209
9.3.5.4. Проверка конфигурации 209
9.3.5.5. Связанные команды 210
9.3.5.6. Пример конфигурации 210
9.3.6. Настройка TTL туннеля 211
9.3.6.1. Результат конфигурации 211
9.3.6.2. Этапы конфигурации 211
9.3.6.3. Проверка конфигурации 211
9.3.6.4. Связанные команды 211
9.3.6.5. Пример конфигурации 211
9.4. Контроль состояния 212
9.4.1. Отображение 212

9.4.2. Отладка 212
10. ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ СЕТЕВЫХ СОЕДИНЕНИЙ 213
10.1. Обзор 213
10.1.1. Протоколы и стандарты 213
10.2. Применение 213
10.2.1. Тестирование связности End-to-End 213
10.2.1.1. Сценарий 213
10.2.1.2. Описание 213
10.2.2. Тест маршрута хоста 214
10.2.2.1. Сценарий 214
10.2.2.2. Описание 214
10.3. Ключевые особенности 214
10.3.1. Обзор 214
10.3.2. Ping-тест 214
10.3.2.1. Принцип работы 214
10.3.2.2. Связанная конфигурация 214
10.3.3. Проверка трассировки 214
10.3.3.1. Принцип работы 214
10.3.3.2. Связанная конфигурация 215
10.4. Настройка 215
10.4.1. Ping-тест 215
10.4.1.1. Результат конфигурации 215
10.4.1.2. Примечания 215
10.4.1.3. Этапы конфигурации 215
10.4.1.4. Проверка конфигурации 215
10.4.1.5. Связанные команды 216
10.4.1.6. Пример конфигурации 219
10.4.2. Проверка трассировки 223
10.4.2.1. Результат конфигурации 223
10.4.2.2. Примечания 223
10.4.2.3. Этапы конфигурации 223
10.4.2.4. Проверка конфигурации 223
10.4.2.5. Связанные команды 223
10.4.2.6. Пример конфигурации 225
11. НАСТРОЙКА TCP 226
11.1. Обзор 226
11.1.1. Протоколы и стандарты 226

11.2. Применение 226
11.2.1. Оптимизация производительности TCP 227
11.2.1.1. Сценарий 227
11.2.1.2. Описание 227
11.2.2. Обнаружение исключения соединения TCP 227
11.2.2.1. Сценарий 227
11.2.2.2. Описание 227
11.3. Ключевые особенности 228
11.3.1. Базовые концепции 228
11.3.2. Обзор 229
11.3.3. Настройка тайм-аута SYN 229
11.3.3.1. Принцип работы 229
11.3.3.2. Связанная конфигурация 229
11.3.4. Настройка размера окна 230
11.3.4.1. Принцип работы 230
11.3.4.2. Связанная конфигурация 230
11.3.5. Настройка сброса отправки пакетов 230
11.3.5.1. Принцип работы 230
11.3.5.2. Связанная конфигурация 230
11.3.6. Настройка MSS 231
11.3.6.1. Принцип работы 231
11.3.6.2. Связанная конфигурация 231
11.3.7. Обнаружение MTU пути 231
11.3.7.1. Принцип работы 231
11.3.7.2. Связанная конфигурация 232
11.3.8. TCP Keepalive 232
11.3.8.1. Принцип работы 232
11.3.8.2. Связанная конфигурация 232
11.4. Настройка 233
11.4.1. Оптимизация производительности TCP 233
11.4.1.1. Результат конфигурации 233
11.4.1.2. Примечания 233
11.4.1.3. Этапы конфигурации 233
11.4.1.4. Проверка конфигурации 234
11.4.1.5. Связанные команды 234
11.4.1.6. Пример конфигурации 236
11.4.2. Обнаружение исключения соединения TCP 236
11.4.2.1. Результат конфигурации 236

11.4.2.2. Этапы конфигурации 236
11.4.2.3. Связанные команды 236
11.4.2.4. Пример конфигурации 237
11.5. Контроль состояния 238
11.5.1. Отображение 238
11.5.2. Отладка 238
12. НАСТРОЙКА ПРОТОКОЛА IPV4/IPV6 REF 240
12.1. Обзор 240
12.2. Применение 240
12.2.1. Балансировка нагрузки 240
12.2.1.1. Сценарий 240
12.2.1.2. Описание 241
12.3. Ключевые особенности 241
12.3.1. Базовые концепции 241
12.3.2. Политики балансировки нагрузки 241
12.3.2.1. Принцип работы 241
12.4. Настройка 241
12.4.1. Отображение статистики пакетов REF 242
12.4.2. Отображение информации о смежности 242
12.4.3. Отображение информации об активном разрешении 242
12.4.4. Отображение информации о пути переадресации пакетов 242
12.4.5. Отображение информации о маршруте в таблице REF 243
13. ОБЩАЯ ИНФОРМАЦИЯ 244
13.1. Гарантия и сервис 244
13.2. Техническая поддержка 244
13.3. Электронная версия документа 244

1. НАСТРОЙКА IP-АДРЕСОВ И СЕРВИСОВ

1.1. Обзор

IP-протокол (Internet Protocol) отправляет пакеты получателю от источника с помощью логических адресов по протоколу IP. На сетевом уровне маршрутизаторы пересылают пакеты на основе IP-адресов.

1.1.1. Протоколы и стандарты

- RFC 1918: распределение адресов в частных IP-сетях.
- RFC 1166: номера в Интернете.

1.2. Применение

Применение	Описание
Настройка IP-адреса для связи	Две подсети обмениваются данными через один интерфейс коммутатора

1.2.1. Настройка IP-адреса для связи

1.2.1.1. Сценарий

Коммутатор подключен к локальной сети (LAN), разделенной на два сегмента сети (подсети), а именно: 172.16.1.0/24 и 172.16.2.0/24. Компьютеры в двух сегментах сети (подсети) могут обмениваться данными с Интернетом через коммутаторы, а между двумя сегментами сети (подсетями) компьютеры могут обмениваться данными друг с другом.

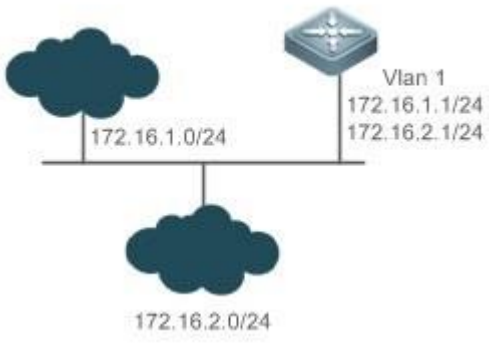


Рисунок 1-1. Настройка IP-адресов

1.2.1.2. Настройка

- Настройте два IP-адреса на VLAN1. Один является основным IP-адресом, а другой — вторичным IP-адресом.
- На хостах в сегменте сети 172.16.1.0/24 установите шлюз на 172.16.1.1; на хостах в подсети 172.16.2.0/24 установите шлюз на 172.16.2.1.

1.3. Ключевые особенности

1.3.1. Базовые концепции

1.3.1.1. IP-адрес

IP-адрес состоит из 32 бит в двоичном формате. Для облегчения написания и описания IP-адрес обычно выражается в десятичной форме. При десятичном делении, IP-адрес делится на четыре группы с восемью битами в каждой группе. Диапазон значений для каждой группы составляет от 0 до 255, а группы разделяются символом ".". Например, 192.168.1.1 — IP-адрес, выраженный в десятичном формате, группы (октеты) разделены точками.

IP-адреса используются для соединения на уровне IP. 32-битный IP-адрес состоит из двух частей: адрес сети и узел. Исходя из значений первых нескольких битов в сетевой части, используемые IP-адреса можно разделить на четыре класса.

Для адреса класса A наиболее значимым битом является 0. 7 бит обозначают идентификатор сети, а 24 бита обозначают локальный адрес. В общей сложности существует 128 сетей класса A.

		8	16 24 32
IP-адрес класса A	0	Network ID	Host ID

Рисунок 1-2.

Для адреса класса B двумя наиболее значимыми битами являются 10. 14 бит обозначают идентификатор сети, а 16 бит обозначают локальный адрес. В общей сложности существует 16 348 сетей класса B.

			8	16 24 32
IP-адрес класса B	1	0	Network ID	Host ID

Рисунок 1-3.

Для адреса класса C наиболее значимыми битами являются первые три бита 110. 21 бит обозначают идентификатор сети, а 8 бит обозначают локальный адрес. В общей сложности существует 2 097 152 сетей класса C.

				8	16 24 32
IP-адрес класса C	1	1	0	Network ID	Host ID

Рисунок 1-4.

Для адреса класса D первые четыре наиболее важных бита — 1110, а другие — адрес многоадресной передачи.

					8 16 24 32
IP-адрес класса D	1	1	1	0	Мультикаст адрес

Рисунок 1-5.

ПРИМЕЧАНИЕ: адреса с первыми четырьмя наиболее значимыми битами 1111 не могут быть назначены. Эти адреса называются адресами класса E и зарезервированы.

Когда IP-адреса планируются во время построения сети, они должны назначаться на основе свойства создаваемой сети. Если сеть должна быть подключена к Интернету, пользователи должны обратиться за IP-адресами к соответствующему агентству. Интернет-корпорация по присвоенным именам и номерам (ICANN) является конечной организацией, ответственной за назначение IP-адресов. Если сеть, которую необходимо создать, является внутренней локальной сетью, пользователям не нужно подавать заявку на IP-адреса. Тем не менее, IP-адреса не могут быть назначены случайным образом. Для работы локальной сети рекомендуется назначать выделенные локальные сетевые адреса, указаны ниже в таблице.

Данная таблица перечисляет зарезервированные и доступные адреса.

Класс	Диапазон адресов	Статус
Сеть класса A	0.0.0.0 - 0.255.255.255	Зарезервированы
	1.0.0.0 - 126.255.255.255	Доступны
	127.0.0.0 - 127.255.255.255	Зарезервированы
Сеть класса B	128.0.0.0 - 191.254.255.255	Доступны
	191.255.0.0 - 191.255.255.255	Зарезервированы
Сеть класса C	192.0.0.0 - 192.0.0.255	Зарезервированы
	192.0.1.0 - 223.255.254.255	Доступны
	223.255.255.0 223.255.255.255	Зарезервированы
Сеть класса D	224.0.0.0 - 239.255.255.255	Мультикаст-адрес
Сеть класса E	240.0.0.0 - 255.255.255.254	Зарезервированы
	255.255.255.255	Широковещательный адрес

Три диапазона адресов предназначены для локальных сетей. Эти адреса не используются в Интернете. Если сети, которым назначены эти адреса, должны быть подключены к Интернету, эти IP-адреса должны быть преобразованы в действительные

интернет-адреса, к примеру, с использованием технологии NAT. В следующей таблице перечислены диапазоны частных адресов. Частные сетевые адреса определены в RFC 1918.

Класс	Диапазон адресов	Статус
Сеть класса A	10.0.0.0 - 10.255.255.255	1 сеть класса A
Сеть класса B	172.16.0.0 - 172.31.255.255	16 сетей класса B
Сеть класса C	192.168.0.0 - 192.168.255.255	256 сетей класса C

Назначение IP-адресов, портов TCP/UDP и других кодов см. в RFC 1166.

1.3.1.2. Маска подсети

Маска подсети также представляет собой 32-разрядное значение. Биты, идентифицируют IP-адрес как сетевой адрес. Биты IP-адреса, соответствующие битам маски подсети, значения которых 1, являются сетевым адресом, а биты IP-адреса, соответствующие битам, значения которых 0, являются адресом хоста. Например, для сетей класса A маска подсети составляет 255.0.0.0. Используя маски подсети, можно разделить сеть на несколько подсетей. Это означает использование некоторых битов адреса хоста в качестве сетевого адреса, что снижает количество хостов и увеличивает количество сетей.

1.3.1.3. Широковещательный (Broadcast) пакет

Широковещательные пакеты относятся к пакетам, предназначенными для всех хостов в физической сети. Оборудование QTECH поддерживает два типа широковещательных пакетов:

1. Широковещательная рассылка, при которой все узлы в указанной сети являются получателями пакетов, а все биты хоста адреса назначения имеют значение равное 1.
2. Ограниченная широковещательная рассылка, при которой все узлы во всех сетях являются получателями пакетов, а все 32 бита адреса назначения имеют значение равное 1.

1.3.1.4. Пакет ICMP

Протокол ICMP (Internet Control Message Protocol) — сетевой протокол в стеке TCP/IP предназначенный для передачи управляющих сообщений между узлами IP и сетевыми устройствами. В основном он используется для уведомления соответствующих устройств о нештатной работе сети.

1.3.1.5. TTL

Time to Live (TTL) — это количество сетевых сегментов (hop-ов), которые пакеты могут пройти до того, как будут отброшены. TTL — это значение в IP-пакете. Он сообщает сети, следует ли отбрасывать пакеты, так как пакеты остаются в сети в течение длительного времени. С каждым шагом, переходом от узла к узлу, значение TTL будет уменьшаться на 1, когда значение TTL станет равным нулю, пакет будет отброшен.

1.3.2. Ключевые особенности

Функция	Описание
IP-адрес	IP-протокол, может работать в интерфейсе только после настройки интерфейса с IP-адресом
Обработка широковещательных (Broadcast) пакетов	Адреса широковещательной рассылки настроены и широковещательные пакеты пересылаются и обрабатываются
Отправка пакетов ICMP	Пакеты ICMP отправляются и принимаются, используются для диагностики сети
Ограничение скорости передачи пакетов ошибок ICMP	Эта функция предотвращает атаки типа "отказ в обслуживании" (DoS)
IP MTU	Настройка максимального размера передаваемого пакета (MTU) для IP-пакетов в интерфейсе
IP TTL	Настройка TTL одноадресных пакетов и широковещательных пакетов
Маршрут источника IP (IP Source routing)	Маршруты источника проверены

1.3.3. IP-адрес

IP-адреса присваиваются интерфейсу следующими способами:

1. Настройка IP-адресов вручную.
2. Получение IP-адресов через DHCP.
3. Получение IP-адресов посредством согласования PPP.
4. Заимствование IP-адресов других интерфейсов.

Эти подходы взаимно исключают друг друга. При настройке нового подхода для получения IP-адреса старый IP-адрес будет перезаписан.

Подробнее о получении IP-адресов через DHCP см. в главе 4 «Настройка DHCP». Далее описаны три других подхода к получению IP-адресов.

1.3.3.1. Настройка IP-адреса для интерфейса

Устройство может получать и отправлять IP-пакеты только после того, как на устройстве настроен IP-адрес. IP-протокол может работать только на интерфейсе, с настроенным IP-адресом.

1.3.3.2. Настройка нескольких IP-адресов для интерфейса

Оборудование QTECH поддерживает конфигурацию с несколькими IP-адресами в одном интерфейсе, один из которых является первичным IP-адресом, а другие —

дополнительными IP-адресами. Теоретически количество дополнительных IP-адресов не ограничено. Однако дополнительные IP-адреса должны принадлежать к разным подсетям, и подсети не должны пересекаться с ранее созданными IP-адресами. При построении сети вторичные IP-адреса часто используются в следующих случаях:

- В сети недостаточно адресов хостов. Например, требуется одна сеть класса C для назначения 254 адресов локальной сети. Однако, если количество хостов превышает 254, одной сети класса C недостаточно, и требуется другая сеть класса C. В этом случае необходимо использовать две сети. Поэтому требуется больше IP-адресов на интерфейсе.
- Многие старые сети основаны на сетях 2-го уровня, объединённых мостами (ethernet bridge), без подсетей. Можно использовать дополнительные IP-адреса для улучшения сети до маршрутизируемой на основе 3-го уровня. Для каждой подсети одно устройство настроено с одним IP-адресом.
- Если две подсети одной сети изолированы другой сетью, можно подключить изолированные подсети, создав подсеть изолированной сети и настроив дополнительный адрес. Одна подсеть не может быть настроена на двух или более интерфейсах устройства.

Получение IP-адресов посредством согласования PPP

ПРИМЕЧАНИЕ: Эта команда поддерживается только в интерфейсах "точка-точка".

Благодаря этой конфигурации интерфейс "точка-точка" принимает IP-адрес, назначенный одноранговым узлом посредством согласования PPP.

Заимствование IP-адресов из другого интерфейса

По умолчанию интерфейс без настроенного IP-адреса. Команда ip unnumbered позволяет заимствовать IP-адрес с другого интерфейса на данном устройстве.

ПРИМЕЧАНИЕ: можно заимствовать IP-адреса интерфейсов Ethernet, интерфейсов туннелей и loopback-интерфейсов. Однако эти интерфейсы не могут заимствовать IP-адреса других интерфейсов.

ПРИМЕЧАНИЕ: заимствованные IP-адреса не могут быть заимствованы на другой интерфейс.

ПРИМЕЧАНИЕ: если заимствованный интерфейс имеет несколько IP-адресов, можно заимствовать только основной IP-адрес.

ПРИМЕЧАНИЕ: IP-адрес одного интерфейса может быть присвоен нескольким интерфейсам.

ПРИМЕЧАНИЕ: заимствованные IP-адреса на интерфейсе всегда согласуются с IP-адресами интерфейса, с которого они были заимствованы.

1.3.3.3. Связанная конфигурация

Настройка интерфейса с одним или более IP-адресами.

- По умолчанию IP-адрес интерфейса не настроен.
- Команда **ip address** используется для настройки IP-адреса интерфейса.
- После настройки IP-адреса и проверки на обнаружение конфликтов интерфейс можно использовать для связи.
- Команда **ip address** *ip-address mask* **secondary** может использоваться для настройки нескольких вторичных IP-адресов.

Получение IP-адреса посредством согласования PPP.

- По умолчанию интерфейс не может получить IP-адрес посредством согласования PPP.
- Команда **ip address negotiate** используется для настройки согласования IP-адреса в интерфейсе "точка-точка".

Заимствование IP-адреса из другого интерфейса.

- По умолчанию IP-адрес интерфейса не настроен.
- Команда **ip unnumbered** может использоваться для заимствования IP-адресов из других интерфейсов.

1.3.4. Обработка широковещательных (Broadcast) пакетов

1.3.4.1. Принцип работы

Broadcast делится на два типа. Один — это ограниченная широковещательная рассылка с IP-адресом — 255.255.255.255. Поскольку рассылка такого типа запрещена маршрутизаторами, она называется широковещательной локальной рассылкой. Другой пример — направленная широковещательная рассылка. Все биты хоста — 1, например, 192.168.1.255/24. Широковещательные пакеты с этими IP-адресами могут быть переданы на маршрутизаторе.

Если IP-сетевые устройства пересылают ограниченные широковещательные пакеты (IP-адрес назначения — 255.255.255.255), сеть может быть перегружена, что сильно влияет на производительность сети. Это обстоятельство называется широковещательным (broadcast) штормом. Устройства предлагают несколько подходов для ограничения широковещательных штормов в локальной сети и предотвращения непрерывного распространения широковещательных штормов. Сетевые устройства второго уровня, такие как мосты и коммутаторы, пересылают и распространяют широковещательные штормы, не имея возможности их отследить.

Лучший способ избежать широковещательного шторма — назначить широковещательный адрес каждой сети для направленной широковещательной рассылки. Для этого IP-протокол должен использовать направленную широковещательную рассылку.

Подробнее о широковещательных штормах см. в RFC 919 и RFC 922.

Направленные широковещательные пакеты относятся к широковещательным пакетам, предназначенными для конкретной подсети. Например, пакеты с адресом назначения 172.16.16.255 называются направленными широковещательными пакетами. Однако, узел, который генерирует этот пакет, не является участником подсети назначения.

После получения направленных широковещательных пакетов устройства, не подключённые напрямую к подсети назначения, пересылают пакеты. После того как направленные широковещательные пакеты достигают устройств, напрямую подключённых к подсети, устройства преобразуют направленные широковещательные пакеты в ограниченные широковещательные пакеты (IP-адрес назначения — 255.255.255.255) и передают пакеты всем узлам в подсети назначения на уровне канала.

1.3.4.2. Связанная конфигурация

Настройка IP-адреса широковещательной рассылки.

- По умолчанию IP-адрес широковещательной рассылки интерфейса составляет 255.255.255.255.
- Чтобы определить широковещательные пакеты других адресов, используйте команду **ip broadcast-address** в режиме конфигурации интерфейса.

Пересылка направленных широковещательных пакетов.

- По умолчанию направленные широковещательные пакеты не могут быть пересланы.
- На указанном интерфейсе можно выполнить команду **ip directed-broadcast**, чтобы включить пересылку пакетов направленной широковещательной рассылки. Таким образом, интерфейс может пересылать направленные широковещательные пакеты в напрямую подключённые сети. Широковещательные пакеты могут передаваться в подсети назначения без влияния на пересылку других пакетов направленной широковещательной рассылки.
- В интерфейсе можно определить список контроля доступа (ACL) для передачи определенных направленных широковещательных пакетов. После определения ACL-списка пересылаются только направленные широковещательные пакеты, соответствующие ACL-списку.

1.3.5. Отправка пакетов ICMP

1.3.5.1. Принцип работы

Сообщение о недоступности протокола ICMP

Устройство получает IP-пакеты, предназначенные ему, и пакеты содержат IP-протокол, который не может быть обработан устройством. Устройство отправляет сообщение о недоступности протокола ICMP на исходный хост. Кроме того, если устройство не знает маршрут для пересылки пакетов, оно также отправляет сообщение о недоступности хоста ICMP.

Сообщение перенаправления ICMP

Иногда маршрут может быть менее оптимальным, поэтому устройство пересылает пакеты с интерфейса, который получает пакеты. Если устройство отправляет пакеты с интерфейса, на котором оно получает пакеты, устройство отправляет ICMP-сообщение о перенаправлении на источник, информируя источник о том, что шлюз является другим устройством в той же подсети. Таким образом, источник отправляет последующие пакеты по оптимальному пути.

Сообщение отклика маски ICMP

Иногда сетевое устройство отправляет сообщение ICMP Address Mask Request для получения маски подсети. Сетевое устройство, получающее данное сообщение, отправляет ответное сообщение ICMP Address Mask Reply.

1.3.5.2. Связанная конфигурация

Включение сообщения о недоступности протокола ICMP.

- По умолчанию функция протокола ICMP сообщение о недоступности включена на интерфейсе.
- Чтобы отключить или включить функцию, можно использовать команду **[no] ip unreachables**

Включение сообщения перенаправления ICMP.

- По умолчанию функция сообщения перенаправления ICMP включена в интерфейсе.
- Вы можете использовать команду [**no**] **ip redirects**, чтобы отключить или включить функцию.

Включение ответного сообщения маски ICMP.

- По умолчанию в интерфейсе включена функция ответа на сообщения ICMP Address Mask Request.

- Можно использовать команду [**no**] **ip mask-reply**, чтобы отключить или включить функцию.

1.3.6. Ограничение скорости передачи пакетов ошибок ICMP

1.3.6.1. Принцип работы

Эта функция ограничивает скорость передачи пакетов ошибок ICMP для предотвращения DoS-атак с помощью алгоритма маркировки контейнера.

Если IP-пакет необходимо фрагментировать, но бит Don't Fragment (DF) в заголовке установлен на 1, устройство отправляет пакет недоступности назначения ICMP (код 4) на хост источника. Этот пакет ошибок ICMP используется для обнаружения MTU-пути. При наличии слишком большого количества других пакетов ошибок ICMP невозможно отправить пакет недоступности назначения ICMP (код 4). В результате происходит сбой функции обнаружения MTU-пути. Чтобы избежать этой проблемы, необходимо ограничить скорость передачи пакетов ICMP с сообщением о недоступности адреса назначения и других ICMP-пакетов ошибок соответственно.

1.3.6.2. Связанная конфигурация

Настройка скорости передачи для с сообщением о недоступности адреса назначения ICMP, инициированных битом DF в IP-заголовке.

- Скорость передачи по умолчанию составляет 10 пакетов каждые 100 мс.
- Команду **ip icmp error-interval DF** можно использовать для настройки скорости передачи.

Настройка скорости передачи других пакетов ошибок ICMP.

- Скорость передачи по умолчанию составляет 10 пакетов каждые 100 мс.
- Команду **ip icmp error-interval** можно использовать для настройки скорости передачи.

1.3.7. IP MTU

1.3.7.1. Принцип работы

Если пакет IP превышает размер IP MTU, программное обеспечение коммутатора фрагментирует пакет. Для всех устройств в одном физическом сегменте сети значение MTU должно быть одинаковым. На оборудовании QTECH можно настроить MTU соединений для интерфейсов. После изменения MTU на интерфейсах будет изменен IP MTU интерфейсов. IP MTU интерфейсов автоматически поддерживает соответствие с MTU интерфейса. Однако при настройке IP MTU интерфейсов значение MTU интерфейсов не изменится, нет обратной автоматической настройки.

1.3.7.2. Связанная конфигурация

Установка IP MTU.

- По умолчанию IP MTU интерфейса составляет 1500.
- Команду **ip mtu** можно использовать для установки MTU пакета IP.

1.3.8. IP TTL

1.3.8.1. Принцип работы

IP-пакет передается с адреса источника на адрес назначения через маршрутизаторы. После установки значения TTL, оно уменьшается на 1 каждый раз при прохождении

IP-пакета через маршрутизатор. Когда значение TTL падает до нуля, маршрутизатор отбрасывает пакет. Это предотвращает бесконечную передачу бесполезных пакетов и потерю пропускной способности.

1.3.8.2. Связанная конфигурация

Установка IP TTL.

- По умолчанию IP TTL интерфейса составляет 64.
- Команду **ip ttl** можно использовать для установки IP TTL интерфейса.

1.3.9. Маршрут источника IP (IP Source routing)

1.3.9.1. Принцип работы

Оборудование QTECH поддерживает IP Source routing. Когда устройство получает IP-пакет, оно проверяет такие опции как source route, loose source route, and record route в заголовке IP-пакета. Эти опции подробно описаны в RFC 791. Если устройство обнаруживает, что в пакете присутствует опция, оно отвечает; если устройство обнаруживает недопустимую опцию, оно отправляет сообщение ICMP об ошибке опции на адрес источника и затем отбрасывает пакет.

После включения Source routing в пакет IP добавляется опция маршрута источника, чтобы проверить пропускную способность определенной сети или помочь пакетам обойти неисправную сеть. Стоит учесть, что этот параметр может привести к сетевым атакам, таким как подмена адреса источника и подмена IP.

1.3.9.2. Связанная конфигурация

Настройка IP Source routing.

- По умолчанию функция IP Source routing включена.
- Команду **ip source-route** можно использовать для включения или отключения функции.

1.4. Настройка

Настройка	Описание и команда	
Настройка IP-адресов интерфейса	(Обязательно) Используется для настройки IP-адреса и разрешения запуска протокола IP в интерфейсе	
	ip address	Вручную настраивает IP-адрес интерфейса
	ip address negotiate	Получает IP-адрес интерфейса посредством согласования PPP
	ip unnumbered	Заимствует IP-адрес из другого интерфейса

Настройка	Описание и команда	
Настройка передачи широковещательной рассылки	(ОПЦИОНАЛЬНО) Используется для установки IP-адреса широковещательной рассылки и включения передачи направленной широковещательной рассылки	
	ip broadcast-address	Настраивает IP-адрес широковещательной рассылки
	ip directed-broadcast	Включает передачу направленной широковещательной рассылки
Настройка пересылки ICMP	(ОПЦИОНАЛЬНО) Используется для включения пересылки пакетов ICMP	
	ip unreachables	Включает сообщения недоступности ICMP и сообщения недоступности хоста
	ip redirects	Включает сообщения перенаправления ICMP
	ip mask-reply	Включает ответные сообщения маски ICMP
Настройка скорости передачи пакетов ошибок ICMP	Опционально	
	ip icmp error-interval DF	Настраивает скорость передачи недостижимых ICMP-пакетов, инициированных битом DF в заголовке IP-адреса
	ip icmp error-interval	Настраивает скорости передачи пакетов ошибок ICMP и пакетов перенаправления ICMP
Установка значения IP MTU	(ОПЦИОНАЛЬНО) Используется для настройки MTU IP в интерфейсе	
	ip mtu	Устанавливает значение IP MTU
Установка значения IP TTL	(ОПЦИОНАЛЬНО) Используется для настройки TTL одноадресных пакетов и широковещательных пакетов	
	ip ttl	Устанавливает значение TTL

Настройка	Описание и команда	
Настройка IP Source routing	(ОПЦИОНАЛЬНО) Используется для проверки источников маршрутов	
	ip source-route	Включает функцию IP source routing

1.4.1. Настройка IP-адресов интерфейса

1.4.1.1. Результат конфигурации

Настройка IP-адреса интерфейса для связности.

1.4.1.2. Этапы конфигурации

Настройка IP-адреса интерфейса.

- ОБЯЗАТЕЛЬНО.
- Выполните настройку в режиме конфигурации интерфейса L3.

Получение IP-адреса интерфейса посредством согласования PPP.

- ОПЦИОНАЛЬНО.
- Если на интерфейсе "точка-точка" не настроен IP-адрес, получите IP-адрес с помощью согласования PPP.
- Выполните настройку в режиме конфигурации интерфейса L3.

Заимствование IP-адресов из другого интерфейса.

- ОПЦИОНАЛЬНО.
- Если на интерфейсе "точка-точка" не настроен IP-адрес, заимствуйте IP-адрес из другого интерфейса.
- Выполните настройку в режиме конфигурации интерфейса L3.

1.4.1.3. Проверка конфигурации

Выполните команду **show ip interface**, чтобы проверить результат.

1.4.1.4. Связанные команды

Настройка IP-адреса интерфейса вручную

Команда	**ip address** *ip-address network-mask* [**secondary**]
Описание параметров	*ip-address*: 32-битный IP-адрес с 8 битами для каждой группы. IP-адрес выражается в десятичном формате, а группы разделяются точкой (.). *network-mask*: 32-битная маска сети. Значение 1 указывает на бит маски, а 0 — на бит хоста. Каждые 8 бит образуют одну группу. Маска сети выражается в десятичном формате, а группы разделяются точкой (.). **secondary**: вторичный IP-адрес

Режим конфигурации	Режим конфигурации интерфейса

Получение IP-адреса интерфейса посредством согласования PPP

Команда	**ip address negotiate**
Режим конфигурации	Режим конфигурации интерфейса

Заимствование IP-адресов из другого интерфейса

Команда	**ip unnumbered** *interface-type interface-number*
Описание параметров	*interface-type*: тип интерфейса. *interface-number*: идентификатор интерфейса
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Unnumbered-интерфейс означает, что интерфейс включен с IP-протоколом без назначенного IP-адреса. Unnumbered-интерфейс должен быть связан с интерфейсом, которому назначен IP-адрес. Для IP-пакета, созданного на unnumbered-интерфейсе, IP-адрес источника пакета является IP-адресом связанного интерфейса. Кроме того, процесс протокола маршрутизации определяет, следует ли отправлять пакет обновления маршрута на unnumbered-интерфейс в соответствии со своим IP-адресом. Если вы хотите использовать unnumbered интерфейс, обратите внимание на следующие ограничения: Интерфейс Ethernet не может быть настроен на unnumbered-интерфейс. Когда последовательный интерфейс инкапсулирует SLIP, HDLC, PPP, LAPB и Frame-Relay, последовательный интерфейс можно настроить на unnumbered-интерфейс. При инкапсуляции посредством relay, только интерфейс "точка-точка" может быть настроен как интерфейс без номера. Интерфейс AnX.25 не может быть настроен как unnumbered-интерфейс. Команда **ping** не может использоваться для проверки правильности работы unnumbered-интерфейса, так как unnumbered-интерфейс не настроен IP-адрес. Однако состояние unnumbered-интерфейса можно отслеживать удаленно с помощью SNMP. Холодный запуск устройства с помощью unnumbered-интерфейса невозможен

1.4.1.5. Пример конфигурации

Настройка IP-адреса для интерфейса.

Этапы конфигурации	Настройте IP-адрес 192.168.23.110 255.255.255.0 на интерфейсе GigabitEthernet 0/0
	QTECH#configure terminal QTECH(config)#interface gigabitEthernet 0/0 QTECH(config-if-GigabitEthernet 0/0)# no switchport QTECH(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
Проверка конфигурации	Выполните команду **show ip interface**, чтобы проверить результат
	QTECH# show ip interface gigabitEthernet 0/0 GigabitEthernet 0/0 IP interface state is: UP IP interface type is: BROADCAST IP interface MTU is: 1500 IP address is: 192.168.23.110/24 (primary)

Получение IP-адреса в интерфейсе "точка-точка" посредством согласования PPP

Этапы конфигурации	Получение IP-адреса в интерфейсе "точка-точка" путем согласования
	QTECH(config)#int virtual-ppp 1 QTECH(config-if-Virtual-ppp 1)#ip address negotiate
Проверка конфигурации	Выполните команду **show run**, чтобы проверить результат
	QTECH#show run interface virtual-ppp 1 Building configuration... Current configuration: 48 bytes interface Virtual-ppp 1 ip address negotiate

1.4.2. Настройка передачи широковещательной рассылки

1.4.2.1. Результат конфигурации

Установите широковещательный адрес интерфейса на 0.0.0.0 и включите передачу направленной широковещательной рассылки.

1.4.2.2. Этапы конфигурации

Настройка IP-адреса широковещательной рассылки.

- (ОПЦИОНАЛЬНО) Некоторые старые хосты могут идентифицировать только широковещательный адрес 0.0.0.0. В этом случае установите широковещательный адрес целевого интерфейса 0.0.0.0.
- Выполните настройку в режиме конфигурации интерфейса L3.

Включение передачи направленной широковещательной рассылки.

- (ОПЦИОНАЛЬНО) Если необходимо разрешить хосту отправлять широковещательные пакеты всем хостам домена, в котором он отсутствует, включите передачу направленной широковещательной рассылки.
- Выполните настройку в режиме конфигурации интерфейса L3.

1.4.2.3. Проверка конфигурации

Выполните команду **show running-config interface**, чтобы проверить результат.

1.4.2.4. Связанные команды

Настройка IP-адреса широковещательной рассылки

Команда	**ip broadcast-address** *ip-address*
Описание параметров	*ip-address*: широковещательный адрес IP-сети
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Обычно адрес назначения широковещательных IP-пакетов составляет все 1, что выражается как 255.255.255.255. Программное обеспечение коммутатора может генерировать широковещательные пакеты с другими IP-адресами посредством определения и принимать собственные широковещательные пакеты и широковещательные пакеты с адресом 255.255.255.255

Разрешение пересылки направленных широковещательных пакетов

Команда	**ip directed-broadcast** [*access-list-number*]
Описание параметров	*access-list-number*: номер списка доступа, в диапазоне от 1 до 199 и от 1300 до 2699. После определения ACL-списка пересылаются только направленные широковещательные пакеты, соответствующие ACL-списку
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Если команда **no ip directed-broadcast** выполняется на интерфейсе, программное обеспечение коммутатора отбрасывает пакеты направленной широковещательной рассылки, полученные из directly connected сети

1.4.2.5. Пример конфигурации

Этапы конфигурации	На интерфейсе GigabitEthernet 0/1 установите адрес назначения пакетов IP широковещательной рассылки на 0.0.0.0 и включите передачу направленной широковещательной рассылки. QTECH#configure terminal QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# no switchport QTECH(config-if-GigabitEthernet 0/1)#ip broadcast-address 0.0.0.0 QTECH(config-if-GigabitEthernet 0/1)#ip directed-broadcast
Проверка конфигурации	Выполните команду **show ip interface**, чтобы проверить результат. QTECH#show running-config interface gigabitEthernet 0/1 ip directed-broadcast ip broadcast-address 0.0.0.0

1.4.3. Настройка пересылки ICMP

1.4.3.1. Результат конфигурации

Включите сообщения ICMP о недоступности, сообщения перенаправления ICMP и Address Mask Reply на интерфейсе.

1.4.3.2. Этапы конфигурации

Включение сообщения ICMP о недоступности.

- По умолчанию сообщения ICMP о недоступности включены.
- (ОПЦИОНАЛЬНО) Команду **no ip unreachables** можно использовать для отключения сообщений о недоступности ICMP.
- Выполните настройку в режиме конфигурации интерфейса L3.

Включение сообщений перенаправления ICMP.

- По умолчанию сообщения перенаправления ICMP включены.
- (ОПЦИОНАЛЬНО) Команду **no ip redirects** можно использовать для отключения сообщений перенаправления ICMP.
- Выполните настройку в режиме конфигурации интерфейса L3.

Включение ответных сообщений о маске ICMP.

- По умолчанию включены сообщения ICMP Address Mask Reply.
- (ОПЦИОНАЛЬНО) Команду **no ip mask-reply** можно использовать для отключения сообщений ICMP Address Mask Reply.
- Выполните настройку в режиме конфигурации интерфейса L3.

1.4.3.3. Проверка конфигурации

Выполните команду **show ip interface**, чтобы проверить результат.

1.4.3.4. Связанные команды

Включение сообщения ICMP о недоступности

Команда	**ip unreachables**
Режим конфигурации	Режим конфигурации интерфейса

Включение сообщений перенаправления ICMP

Команда	**ip redirects**
Режим конфигурации	Режим конфигурации интерфейса

Включение ICMP Address Mask Reply

Команда	**ip mask-reply**
Режим конфигурации	Режим конфигурации интерфейса

1.4.3.5. Пример конфигурации

Этапы конфигурации	Включите сообщения ICMP о недоступности, сообщения перенаправления ICMP и ICMP Address Mask Reply на интерфейсе gigabitEthernet 0/1
	QTECH#configure terminal QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# no switchport

	QTECH(config-if-GigabitEthernet 0/1)# ip unreachables QTECH(config-if-GigabitEthernet 0/1)# ip redirects QTECH(config-if-GigabitEthernet 0/1)# ip mask-reply
Проверка конфигурации	Выполните команду **show ip interface**, чтобы проверить результат
	QTECH#show ip interface gigabitEthernet 0/1 GigabitEthernet 0/1 ICMP mask reply is: ON Send ICMP redirect is: ON Send ICMP unreachabled is: ON

1.4.4. Настройка скорости передачи пакетов ошибок ICMP

1.4.4.1. Результат конфигурации

Настройка скорости передачи пакетов ошибок ICMP.

1.4.4.2. Этапы конфигурации

Настройка скорости передачи для пакетов ICMP Destination Unreachable, инициированных битом DF в IP-заголовке.

- ОПЦИОНАЛЬНО.
- Выполните настройку в режиме глобальной конфигурации.

Настройка скорости передачи пакетов других ошибок ICMP.

- ОПЦИОНАЛЬНО.
- Выполните настройку в режиме глобальной конфигурации.

1.4.4.3. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить результат.

1.4.4.4. Связанные команды

Настройка скорости передачи для пакетов ICMP Destination Unreachable, инициированных битом DF в IP-заголовке

Команда	**ip icmp error-interval DF** *milliseconds* [*bucket-size*]
Описание параметров	*milliseconds*: цикл обновления контейнера токенов. Диапазон значений составляет от 0 до 2 147 483 647, а значение по умолчанию составляет 100 мс. Если значение равно 0, скорость передачи пакетов ошибок ICMP не ограничена. *bucket-size*: количество токенов, содержащихся в контейнере токенов. Диапазон значений составляет от 1 до 200, а значение по умолчанию — 10

Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Эта функция ограничивает скорость передачи пакетов ошибок ICMP для предотвращения DoS-атак с помощью алгоритма контейнера токенов. Если IP-пакет необходимо фрагментировать, но бит DF в заголовке установлен на 1, устройство отправляет пакет ICMP destination unreachable (код 4) на хост источника. Этот код ICMP используется для обнаружения MTU по пути следования. При наличии слишком большого количества других пакетов ошибок ICMP невозможно отправить пакет ICMP destination unreachable (код 4). В результате происходит сбой функции обнаружения MTU по пути следования. Чтобы избежать этой проблемы, необходимо ограничить скорость передачи пакетов destination unreachable и других ICMP-пакетов ошибок соответственно. Рекомендуется установить для процесса обновления число кратное 10 мс. Если для процесса обновления установлено значение больше 0 и меньше 10 мс, то фактически происходит обновление длительностью 10 мс. Например, если частота обновления установлена на одно обновление за 5 мс, фактическая частота обновления составляет 2 обновления за 10 мс. Если цикл обновления не является кратным 10 мс, то фактически вступающий в силу цикл обновления автоматически преобразуется в кратный 10 мс. Например, если частота обновления установлена на 3 обновления за 15 мс, фактическая частота обновления составляет 2 обновления за 10 мс

Настройка скорости передачи других пакетов ошибок ICMP

Команда	**ip icmp error-interval** *milliseconds* [*bucket-size*]
Описание параметров	*milliseconds*: цикл обновления контейнера токенов. Диапазон значений: от 0 до 2 147 483 647, а значение по умолчанию — 100 (мс). Если значение равно 0, скорость передачи пакетов ошибок ICMP не ограничена. *bucket-size*: количество токенов, содержащихся в контейнере токенов. Диапазон значений составляет от 1 до 200, а значение по умолчанию — 10
Режим конфигурации	Режим глобальной конфигурации

Встроенная подсказка	Эта функция ограничивает скорость передачи пакетов ошибок ICMP для предотвращения DoS-атак с помощью алгоритма контейнера токенов. Рекомендуется установить для процесса обновления число кратное 10 мс. Если для процесса обновления установлено значение больше 0 и меньше 10 мс, то фактически происходит обновление длительностью 10 мс. Например, если частота обновления установлена на одно обновление за 5 мс, фактическая частота обновления составляет 2 обновления за 10 мс. Если цикл обновления не является кратным 10 мс, то фактически вступающий в силу цикл обновления автоматически преобразуется в кратный 10 мс. Например, если частота обновления установлена на 3 обновления за 15 мс, фактическая частота обновления составляет 2 обновления за 10 мс

1.4.4.5. Пример конфигурации

Этапы конфигурации	Установите скорость передачи пакетов ICMP destination unreachable, для которых активирован бит DF в IP-заголовке до 100 пакетов в секунду, а скорость передачи других пакетов ошибок ICMP до 10 пакетов в секунду
	QTECH(config)# ip icmp error-interval DF 1000 100 QTECH(config)# ip icmp error-interval 1000 10
Проверка конфигурации	Выполните команду **show running-config**, чтобы проверить результат
	QTECH#show running-config | include ip icmp error-interval ip icmp error-interval 1000 10 ip icmp error-interval DF 1000 100

1.4.5. Установка значения IP MTU

1.4.5.1. Результат конфигурации

Настройте IP MTU пакета.

1.4.5.2. Этапы конфигурации

- (ОПЦИОНАЛЬНО) Если IP MTU взаимосвязанных интерфейсов отличается от устройств в одном физическом сегменте сети, установите для IP MTU одинаковое значение.
- Выполните настройку в режиме конфигурации интерфейса L3.

1.4.5.3. Проверка конфигурации

Выполните команду **show ip interface**, чтобы проверить результат.

1.4.5.4. Связанные команды

Установка значения IP MTU

Команда	**ip mtu** *bytes*
Описание параметров	*bytes*: IP MTU пакета. Диапазон значений от 68 до 1500 байт
Режим конфигурации	Режим конфигурации интерфейса

1.4.5.5. Пример конфигурации

Этапы конфигурации	Установите для параметра MTU IP-интерфейса GigabitEthernet 0/1 значение 512 Б
	QTECH#configure terminal QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# no switchport QTECH(config-if-GigabitEthernet 0/1)#ip mtu 512
Проверка конфигурации	Выполните команду **show ip interface**, чтобы проверить результат
	QTECH# show ip interface gigabitEthernet 0/1 IP interface MTU is: 512

1.4.6. Установка значения IP TTL

1.4.6.1. Результат конфигурации

Изменяет значение TTL IP-интерфейса.

1.4.6.2. Этапы конфигурации

- ОПЦИОНАЛЬНО.
- Выполните настройку в режиме конфигурации интерфейса L3.

1.4.6.3. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить результат.

1.4.6.4. Связанные команды

Установка значения IP TTL

Команда	**ip ttl** *value*
Описание параметров	*value*: значение TTL. Диапазон значений от 0 до 255
Режим конфигурации	Режим глобальной конфигурации

1.4.6.5. Пример конфигурации

Этапы конфигурации	Установите TTL одноадресных пакетов на 100
	QTECH#configure terminal QTECH(config)#ip ttl 100
Проверка конфигурации	Выполните команду **show running-config**, чтобы проверить результат
	QTECH#show running-config ip ttl 100

1.4.7. Настройка IP Source routing

1.4.7.1. Результат конфигурации

Включение или отключение функции IP Source routing.

1.4.7.2. Этапы конфигурации

- По умолчанию функция IP Source routing включена.
- (ОПЦИОНАЛЬНО) Команду **no ip source-route** можно использовать для отключения функции IP Source routing.

1.4.7.3. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить результат.

1.4.7.4. Связанные команды

Настройка IP Source routing

Команда	**ip source-route**
Режим конфигурации	Режим глобальной конфигурации

1.4.7.5. Пример конфигурации

Этапы конфигурации	Включает функцию маршрута источника IP
	QTECH#configure terminal QTECH(config)#no ip source-route
Проверка конфигурации	Выполните команду **show running-config**, чтобы проверить результат
	QTECH#show running-config no ip source-route

1.5. Контроль состояния

1.5.1. Отображение

Описание	Команда
Отображает IP-адрес интерфейса	**show ip interface** [interface-typeinterface-number | brief]
Отображает таблицу пересылки	**show ip route** [address [mask]]
Отображает статистику таблицы пересылки	**show ip route summary**
Отображает статистику IP-пакетов	**show ip packet statistics** [total | interface-name]

2. НАСТРОЙКА ARP

2.1. Обзор

В локальной сети (LAN) каждое сетевое устройство IP имеет два адреса:

1. Локальный адрес (MAC-адрес). Поскольку локальный адрес содержится в заголовке кадра уровня канала данных (L2), это адрес L2. Тем не менее, он обрабатывается подуровнем MAC на L2 и, таким образом, обычно называется MAC-адресом. MAC-адреса представляют сетевые устройства IP в локальных сетях.
2. Сетевой адрес. Сетевые адреса в Интернете представляют собой сетевые устройства IP, а также указывают сети, в которых находятся устройства.

В локальной сети два IP-устройства могут взаимодействовать друг с другом только после того, как будут изучены 48-битные MAC-адреса обоих устройств. Процесс получения MAC-адреса на основе IP-адреса называется ARP (address resolution protocol). Существует два типа протоколов разрешения адресов: 1) Протокол определения адреса (ARP); 2) прозрачный (proxy) ARP.

ARP и прозрачный (proxy) ARP описаны соответственно в RFC 826 и RFC 1027.

Протокол ARP используется для привязки MAC-адреса к IP-адресу. При вводе IP-адреса можно узнать соответствующий MAC-адрес через ARP. После получения MAC-адреса сопоставление IP-MAC будет сохранено в кеше ARP сетевого устройства. С помощью MAC-адреса IP-устройство может инкапсулировать кадры L2 и отправлять их в локальную сеть. По умолчанию пакеты IP и ARP на уровне Ethernet инкапсулируются в кадры Ethernet.

2.1.1. Протоколы и стандарты

- RFC 826: протокол преобразования адресов Ethernet (ARP)
- RFC 1027: использование протокола ARP для внедрения прозрачных шлюзов подсети

2.2. Применение

Применение	Описание
ARP в локальной сети	Пользователь запоминает MAC-адреса других пользователей в том же сегменте сети через ARP
Прозрачная передача на основе протокола Proxy ARP	С помощью прозрачного (proxy) протокола ARP пользователь может напрямую связываться с пользователями в другой сети, не зная, что она существует

2.2.1. ARP в локальной сети

2.2.1.1. Сценарий

Протокол ARP требуется во всех локальных сетях IPv4.

- Пользователю необходимо узнать MAC-адреса других пользователей с помощью протокола ARP, чтобы установить с ними связь.

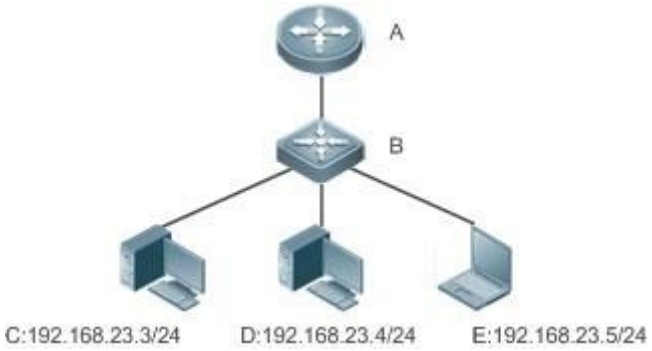


Рисунок 2-1.

A — это маршрутизатор.

B — коммутатор. Он действует как шлюз.

C, D и E являются хостами.

2.2.1.2. Описание

Включите протокол ARP в локальной сети, чтобы реализовать сопоставление IP-MAC.

2.2.2. Прозрачная передача на основе протокола Proxy ARP

2.2.2.1. Сценарий

Выполняется прозрачная передача данных через сеть IPv4 LAN.

- Включите Proxy ARP на маршрутизаторе, чтобы обеспечить прямую связь между пользователями в разных сегментах сети.

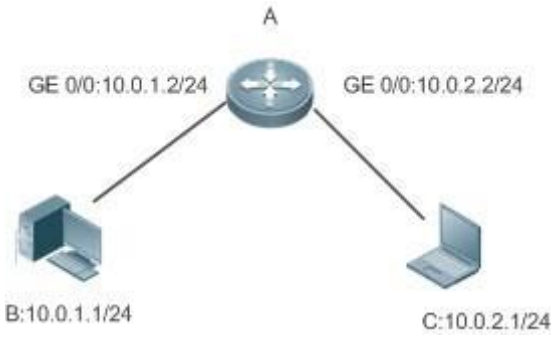


Рисунок 2-2.

A — это маршрутизатор, соединяющий две LAN.

B и C являются хостами в разных подсетях. Для них не настроен шлюз по умолчанию.

2.2.2.2. Описание

Включите Proxy ARP на шлюзе подсети. После настройки шлюз может выступать в качестве proxy-сервера для подключения хоста без информации о маршруте и для получения MAC-адресов IP-пользователей в других подсетях.

2.3. Ключевые особенности

2.3.1. Обзор

Функция	Описание
Статический ARP	Пользователи могут вручную указать сопоставление IP-MAC, чтобы предотвратить распознавание устройством неверных записей ARP
Атрибуты ARP	Пользователи могут указать тайм-аут записи ARP, время и интервал повторной передачи запроса ARP, а также максимальное количество неразрешенных записей ARP
Trusted ARP	Trusted протокол ARP используется для предотвращения подмены ARP
Gratuitous ARP	Gratuitous ARP используется для обнаружения конфликтов IP-адресов и разрешения периферийным устройствам обновлять записи ARP
Proxy ARP	Proxy-сервер отвечает на запросы ARP от других устройств в разных подсетях
Local Proxy ARP	Proxy-сервер отвечает на запросы ARP от других устройств в той же подсети
Определение надежности ARP	Обнаружение недоступных соседних узлов (NUD) используется для того, чтобы убедиться в том, что правильном изучении записей ARP
IP Guard на основе ARP	Можно задать количество IP-пакетов для запуска отброса ARP, чтобы предотвратить отправку на CPU большого количества неизвестных одноадресных (unknown unicast) пакетов
Преобразование запросов ARP в запросы аутентификации VLAN	Устройство не передает широковещательные запросы ARP в запросы аутентификации VLAN, чтобы сократить количество широковещательных запросов ARP в сети

2.3.2. Статический ARP

Статические записи ARP могут быть настроены вручную или назначены сервером аутентификации. Настроенные вручную записи приоритетнее. Статический ARP может предотвратить обучение устройством неверных записей ARP.

2.3.2.1. Принцип работы

Если настроены статические записи ARP, устройство не выполняет активное обновление записей ARP, и эти записи ARP существуют постоянно.

Когда устройство пересылает пакеты уровня 3, статический MAC-адрес инкапсулируется в заголовок Ethernet в качестве MAC-адреса назначения.

2.3.2.2. Связанная конфигурация

Включение статического ARP.

Выполните команду **arp** [**vrf** *name*] *ip-address mac-address type* в режиме глобальной конфигурации, чтобы настроить статические записи ARP. По умолчанию статическая запись ARP не настроена. Пользователи могут связать статические записи ARP с отдельными объектами VRF или глобальным объектом VRF. Инкапсуляция ARP поддерживает только тип Ethernet II, который представлен ARPA.

2.3.3. Атрибуты ARP

Пользователи могут указать тайм-аут ARP, интервал и время повторной передачи запроса ARP, а также максимальное количество записей ARP на интерфейсе.

2.3.3.1. Принцип работы

Тайм-аут ARP

Тайм-аут ARP применяется только к динамически обученным сопоставлениям IPMAC. По истечении времени ожидания записи ARP устройство отправляет пакет одноадресного ARP-запроса, чтобы определить, находится ли конец однорангового узла в оперативном режиме. Если он получает ответ ARP со стороны узла, он не удаляет эту запись ARP. В противном случае устройство удалит данную запись ARP.

Если для параметра ARP timeout задано меньшее значение, таблица сопоставления, хранящаяся в кеш ARP, более точна, но ARP потребляет больше пропускной способности сети.

Интервал и время повторной передачи запроса ARP

Устройство последовательно отправляет запросы ARP для разрешения IP-адреса на MAC-адрес. Чем короче интервал повторной передачи, тем быстрее работает протокол. Чем больше раз выполняется повторная передача запроса ARP, тем больше вероятность успешного решения и тем больше будет потреблять полоса пропускания ARP.

Максимальное количество неразрешенных записей ARP

В локальной сети атаки ARP и сканирование могут привести к появлению большого количества неразрешенных записей ARP, генерируемых шлюзом. В результате шлюз не может обучаться MAC-адресам пользователей. Чтобы предотвратить такие атаки, пользователи могут настроить максимальное количество неразрешенных записей ARP.

2.3.3.2. Связанная конфигурация

Настройка тайм-аута ARP

Запустите команду **arp timeout** *seconds* в режиме конфигурации интерфейса, чтобы настроить тайм-аут ARP. По умолчанию тайм-аут составляет 3600 секунд. Вы можете изменить его в зависимости от ситуации.

Настройка интервала и времени повторной передачи запроса ARP.

- Выполните команду **arp retry interval** *seconds* в режиме глобальной конфигурации, чтобы настроить интервал повторной передачи запроса ARP. Интервал по умолчанию составляет 1 секунду. Вы можете изменить его в зависимости от ситуации.

- Выполните команду **arp retry times** *number* в режиме глобальной конфигурации, чтобы настроить время повторной передачи запроса ARP. По умолчанию время повторной передачи равно 5. Вы можете изменить его в зависимости от ситуации.

Настройка максимального количества неразрешенных записей ARP.

Выполните команду **arp unresolve** *number* в режиме глобальной конфигурации, чтобы настроить максимальное количество неразрешенных записей ARP. Значение по умолчанию — максимальное количество записей ARP, поддерживаемых устройством. Вы можете изменить его в зависимости от ситуации.

2.3.4. Trusted ARP

2.3.4.1. Принцип работы

В качестве типа специальных записей ARP в таблицу ARP добавляются доверенные записи ARP для предотвращения подделки ARP. Доверенные записи ARP имеют характеристики как статических, так и динамических записей ARP, с приоритетом выше, чем у динамических записей ARP и ниже, чем у статических записей ARP. Trusted ARP имеет механизм устаревания, аналогичный механизму динамического ARP. Когда запись ARP устареет, устройство активно отправляет пакет запроса ARP, чтобы определить, существует ли соответствующий пользователь. Если пользователь отправляет ответ, устройство считает пользователя активным и обновляет тайм-аут ARP. В противном случае устройство удалит запись ARP. Trusted ARP имеет характеристики статического ARP, то есть устройство не запоминает пакеты ARP для обновления MAC-адреса и идентификатора интерфейса в записи ARP.

Когда пользователь переходит в оперативный режим, сервер аутентификации получает надежное сопоставление IP-MAC пользователя через коммутатор доступа и добавляет доверенные записи ARP в шлюз пользователя. Этот процесс прозрачен для сетевого администратора и не влияет на работу администратора по управлению сетью.

Так как доверенные записи ARP поступают из подлинных источников и не обновляются, они могут эффективно предотвратить подделку ARP, нацеленную на шлюз.

2.3.4.2. Связанная конфигурация

Включение trusted ARP.

- Запустите команду **service trustedarp** в режиме глобальной конфигурации, чтобы включить trusted ARP. Данная функция выключена по умолчанию.
- Выполните команду **arp trusted user-vlan** *vid1* **translated-vlan** *vid2* для доверенного пользователя в режиме глобальной конфигурации, чтобы реализовать перенаправление VLAN. Данная функция выключена по умолчанию. Если виртуальная локальная сеть, которую выдвинул сервер, отличается от VLAN в доверенной записи ARP, пользователям необходимо включить перенаправление VLAN.
- Запустите команду **arp trusted aging** в режиме глобальной конфигурации, чтобы включить устаревание ARP. По умолчанию доверенные записи ARP не устаревают.
- Запустите команду **arp trusted number** в режиме глобальной конфигурации, чтобы настроить емкость доверенных записей ARP. Значение по умолчанию равно половине общей емкости записей ARP. Вы можете изменить его в зависимости от ситуации.

2.3.5. Gratuitous ARP

2.3.5.1. Принцип работы

Пакеты Gratuitous ARP представляют собой особый тип пакетов ARP. В Gratuitous ARP-пакете IP-адреса источника и назначения являются IP-адресами локального устройства. Gratuitous ARP-пакеты имеют два назначения:

1. Обнаружение конфликтов IP-адресов. Если устройство получает Gratuitous ARP-пакет и обнаруживает, что IP-адрес в пакете такой же, как и его собственный IP-адрес, оно отправляет ответ ARP, чтобы уведомить другое устройство о конфликте IP-адресов.
2. Обновление ARP. При изменении MAC-адреса на интерфейсах устройство отправляет Gratuitous ARP-пакет для уведомления других устройств для обновления записей ARP.

Устройство может получать Gratuitous ARP-пакеты. После получения непроверенного ARP-пакета устройство проверяет, существует ли соответствующая динамическая запись ARP. Если да, устройство обновляет запись ARP на основе информации, содержащейся в Gratuitous ARP.

2.3.5.2. Связанная конфигурация

Включение Gratuitous ARP.

Запустите команду **arp gratuitous-send interval** *seconds* [*number*] в режиме конфигурации интерфейса, чтобы включить Gratuitous ARP. По умолчанию эта функция отключена на интерфейсах. Обычно эту функцию необходимо включить в интерфейсе шлюза, чтобы периодически обновлять MAC-адрес шлюза на нижестоящих устройствах, что предотвращает подделку шлюза другими пользователями.

2.3.6. Proxy ARP

2.3.6.1. Принцип работы

Включение протокола Proxy ARP, может помочь хосту без информации о маршруте получить MAC-адреса пользователей IP в других подсетях. Например, если устройство, получающее запрос ARP, находит исходный IP-адрес в другом сегменте сети от IP-адреса назначения и знает маршрут до адреса назначения, устройство отправляет ответ ARP, содержащий собственный MAC-адрес Ethernet. Вот так работает Proxy ARP.

2.3.6.2. Связанная конфигурация

Включение Proxy ARP.

- Запустите команду **ip proxy-arp** в режиме конфигурации интерфейса, чтобы включить Proxy ARP.
- Данная функция выключена по умолчанию.

2.3.7. Local Proxy ARP

2.3.7.1. Принцип работы

Протокол Local Proxy ARP позволяет устройству выступать в качестве Local Proxy ARP в локальной сети VLAN (общей сети VLAN или подсети VLAN).

После включения протокола Local Proxy ARP устройство может помочь пользователям получить MAC-адреса других пользователей в той же подсети. Например, если на устройстве включена защита портов, пользователи, подключенные к разным портам,

изолируются на уровне 2. После включения протокола Local Proxy устройство, получающее запрос ARP, выступает в качестве Local Proxy ARP-сервера для отправки ответа ARP, содержащего собственный MAC-адрес Ethernet. В этом случае разные пользователи взаимодействуют друг с другом по маршрутам уровня 3. Вот так работает протокол Local Proxy ARP.

2.3.7.2. Связанная конфигурация

Включение протокола Local Proxy ARP.

- Запустите команду **local-proxy-arp** в режиме конфигурации интерфейса, чтобы включить Local Proxy ARP.
- Данная функция выключена по умолчанию.
- Эта команда поддерживается только на виртуальных интерфейсах коммутатора (SVI).

2.3.8. Определение надежности ARP

2.3.8.1. Принцип работы

Команда **arp trust-monitor enable** используется для включения функционала anti-ARP spoofing, чтобы предотвратить попадание излишних бесполезных записей ARP в ресурсы устройства. После включения определения надежности ARP на интерфейсе 3 уровня, устройство получает с этого интерфейса пакеты запросов ARP:

Если соответствующая запись не существует, устройство создает динамическую запись ARP и выполняет NUD через 1–5 секунд. То есть, устройство начинает выполнять устаревание недавно выученных записей ARP и отправляет Unicast-запрос ARP. Если устройство получает пакет обновления ARP от однорангового узла в течение срока устаревания, оно сохраняет запись. В противном случае запись будет удалена.

Если соответствующая запись ARP существует, NUD не выполняется.

Если MAC-адрес в существующей записи динамического ARP обновлен, устройство также выполняет NUD.

Поскольку эта функция добавляет строгую процедуру подтверждения в процесс обучения ARP, она влияет на эффективность обучения ARP.

После отключения этой функции NUD не требуется для обучения и обновления записей ARP.

2.3.8.2. Связанная конфигурация

Включение обнаружения trusted ARP.

Выполните команду **arp trust-monitor enable** в режиме конфигурации интерфейса, чтобы включить определение надежности ARP. Данная функция выключена по умолчанию.

2.3.9. IP Guard на основе ARP

2.3.9.1. Принцип работы

При получении IP-пакетов, адрес назначения которых неизвестен, коммутатор не может пересылать их и, следовательно, должен отправить их на ЦП для разрешения адресов. При отправке большого количества таких пакетов на ЦП процессор будет перегружен, что повлияет на другие службы коммутатора.

После включения IP Guard на основе ARP, коммутатор, получающий пакеты запроса ARP, подсчитывает количество пакетов, в которых IP-адрес назначения попадает в эту запись

ARP. Если это число равно настроенному числу, коммутатор устанавливает запись об устройстве в аппаратном обеспечении, чтобы оборудование не передало пакеты с этим IP-адресом назначения на ЦП. По завершении разрешения адреса коммутатор продолжает пересылать пакеты с этим IP-адресом назначения.

2.3.9.2. Связанная конфигурация

Включение IP Guard на основе ARP.

- Выполните команду **arp anti-ip-attack** в режиме глобальной конфигурации, чтобы настроить количество IP-пакетов для запуска сброса ARP.
- По умолчанию коммутатор отбрасывает соответствующую запись ARP после получения трех неизвестных одноадресных пакетов, содержащих один и тот же IP-адрес назначения.

2.3.10. Преобразование запросов ARP в запросы аутентификации VLAN

2.3.10.1. Принцип работы

В режиме аутентификации шлюза все подсети в Super VLAN по умолчанию являются VLAN аутентификации. Пользователи в сети аутентификации VLAN должны пройти аутентификацию для доступа к сети. После аутентификации на устройстве создается статическая запись ARP. Поэтому при доступе к аутентифицированному пользователю устройству не нужно отправлять запросы ARP в VLAN аутентификации. Если устройство пытается получить доступ к пользователям в VLAN с исключением аутентификации, ему нужно отправлять запросы ARP только в VLAN с исключением аутентификации.

В режиме аутентификации шлюза эта функция включена на устройстве по умолчанию. Если устройству требуется доступ к пользователям с исключениями в сети аутентификации VLAN, отключите эту функцию.

2.3.10.2. Связанная конфигурация

Преобразование запросов ARP в запросы аутентификации VLAN.

- Запустите команду **arp suppress-auth-vlan-req** в режиме конфигурации интерфейса, чтобы не отправлять запросы ARP в сети аутентификации VLAN.
- Данная функция включена по умолчанию.

2.4. Настройка

Настройка	Описание и команда	
Включение статического ARP	(ОПЦИОНАЛЬНО) Используется для включения статической привязки IP-MAC	
	arp	Включение статического ARP
Настройка атрибутов ARP	Пользователи могут указать тайм-аут ARP, интервал и время повторной передачи запроса ARP, а также максимальное количество неразрешенных записей ARP	
	arp timeout	Настройка тайм-аут ARP

Настройка	Описание и команда	
Настройка атрибутов ARP	**arp retry interval**	Настройка интервал повторной передачи запроса ARP
	arp unresolve	Настройка максимального количества неразрешенных записей ARP
Включение trusted ARP	(ОПЦИОНАЛЬНО) Используется для защиты от подделки ARP	
	service trustedarp	Включение доверенного ARP
	arp trusted user-vlan	Включение перенаправления VLAN при добавлении доверенной записи ARP
	arp trusted aging	Включение доверенного устаревания ARP
	arp trusted	Настройка емкости доверенных записей ARP
Включение Gratuitous ARP	(ОПЦИОНАЛЬНО) Используется для обнаружения конфликтов IP-адресов и позволяет периферийным устройствам обновлять записи ARP	
	arp gratuitous-send interval	Включение Gratuitous ARP
Ошибка! сточник ссылки не найден.	(ОПЦИОНАЛЬНО) Используется для выполнения функции прозрачного (proxy) сервера для ответа на запросы ARP от устройств в различных подсетях	
	ip proxy-arp	Включение Proxy ARP
Ошибка! сточник ссылки не найден.	(ОПЦИОНАЛЬНО) Используется для выполнения функции прозрачного (proxy) сервера для ответа на запросы ARP от других устройств в той же подсети	
	local-proxy-arp	Включение Local Proxy ARP

Настройка	Описание и команда	
Ошибка! сточник ссылки не найден.	(ОПЦИОНАЛЬНО) Используется для одноадресной рассылки пакетов ARP-запросов, чтобы убедиться в том, что правильно введены записи ARP	
	arp trusted-monitor enable	Включение определения надежности ARP
Включение защиты IP-адресов на основе ARP	(ОПЦИОНАЛЬНО) Используется для предотвращения отправки большого количества IP-пакетов на ЦП	
	arp anti-ip-attack	Настройка количества IP-пакетов для запуска сброса ARP
Преобразование запросов ARP в запросы аутентификации VLAN	(ОПЦИОНАЛЬНО) Используется для того, чтобы не отправлять запросы ARP в сети аутентификации VLAN	
	arp suppress-auth-vlan-req	Преобразование запросов ARP в запросы аутентификации VLAN

2.4.1. Включение статического ARP

2.4.1.1. Результат конфигурации

Пользователи могут вручную указать сопоставление IP-MAC, чтобы предотвратить распознавание устройством неверных записей ARP.

2.4.1.2. Примечания

После настройки статической записи ARP коммутатор L3 запоминает физический порт, соответствующий MAC-адресу в статической записи ARP, прежде чем выполнять маршрутизацию.

2.4.1.3. Этапы конфигурации

Настройка статических записей ARP.

- Опционально.
- Можно настроить статическую запись ARP для привязки IP-адреса устройства восходящего потока к его MAC-адресу, чтобы предотвратить изменение MAC-адреса, вызванное атаками ARP.
- Настройка статических записей ARP производится в режиме глобальной конфигурации.

2.4.1.4. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить результат. Или запустите **show arp static**, чтобы проверить, создана ли таблица кеша статического ARP.

2.4.1.5. Связанные команды

Настройка статических записей ARP.

Команда	**arp** [**vrf** *name* | **oob**] *ip-address mac-address type*
Описание параметров	**vrf** *name*: указывает объект VRF. Параметр *name* указывает имя объекта VRF. **oob**: настраивает статическую запись ARP для Management-порта. *ip-address*: указывает IP-адрес, сопоставленный с MAC-адресом, который имеет четырехточечный десятичный формат. *mac-address*: указывает адрес L2, состоящий из 48 бит. *type*: указывает тип инкапсуляции ARP. Для интерфейса Ethernet ключевое слово **arpa**
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Коммутатора запрашивает 48-битный MAC-адрес на основе 32-битного IP-адреса в таблице кеша ARP. Поскольку большинство хостов поддерживают динамическое разрешение ARP, обычно статическое сопоставление ARP не настроено. Используйте команду **clear arp-cache** для очистки динамических записей ARP

2.4.1.6. Пример конфигурации

Сценарий	Топологию сети (Рисунок 2-1)
Этапы конфигурации	Настройте статическую запись ARP на B, чтобы статически связать IP-адрес A с MAC-адресом. QTECH(config)#arp 192.168.23.1 001F.CE22.334B arpa
Проверка конфигурации	Запустите команду **show arp static**, чтобы отобразить статическую запись ARP. QTECH(config)#show arp static Protocol Address Age(min) Hardware Type Interface Internet 192.168.23.1 <static> 001F.CE22.334B arpa 1 static arp entries exist

2.4.1.7. Типичные ошибки

Неверный MAC-адрес в статическом ARP.

2.4.2. Настройка атрибутов ARP

2.4.2.1. Результат конфигурации

Пользователи могут указать тайм-аут ARP, интервал и время повторной передачи запроса ARP, а также максимальное количество неразрешенных записей ARP.

2.4.2.2. Этапы конфигурации

Настройка тайм-аута ARP.

- Опционально.
- В локальной сети, если пользователь часто переходит в online/offline режим, рекомендуется установить малое время ожидания ARP для удаления некорректных записей ARP как можно скорее.
- Настройте тайм-аут ARP в режиме конфигурации интерфейса.

Настройка интервала и времени повторной передачи запроса ARP.

- Опционально.
- Если сетевые ресурсы недостаточны, рекомендуется установить интервал повторной передачи запроса ARP большим, а время повторной передачи малым, чтобы снизить потребление пропускной способности сети.
- Настройте интервал и время повторной передачи запроса ARP в режиме глобальной конфигурации.

Настройка максимального количества неразрешенных записей ARP.

- Опционально.
- Если сетевых ресурсов недостаточно, рекомендуется установить максимальное количество неразрешенных записей ARP, чтобы снизить потребление полосы пропускания сети.
- Настройте максимальное количество неразрешенных записей ARP в режиме глобальной конфигурации.

2.4.2.3. Проверка конфигурации

Запустите команду **show arp timeout** для отображения тайм-аута всех интерфейсов.

Выполните команду **show running-config**, чтобы отобразить интервал и время повторной передачи запроса ARP, а также максимальное количество неразрешенных записей ARP.

2.4.2.4. Связанные команды

Настройка тайм-аута ARP

Команда	**arp timeout** *seconds*
Описание параметров	*seconds*: указывает время ожидания в секундах в диапазоне от 0 до 2 147 483. Значение по умолчанию: 3600
Режим конфигурации	Режим конфигурации интерфейса

Встроенная подсказка	Тайм-аут ARP применяется только к динамическим сопоставлениям IP-MAC. Чем меньше значение ARP timeout, тем точнее таблица сопоставления, хранящаяся в кеш ARP, но ARP потребляет больше пропускной способности сети

Настройка интервала и времени повторной передачи запроса ARP

Команда	**arp retry interval** *seconds*
Описание параметров	*seconds*: указывает интервал повторной передачи запроса ARP в секундах в диапазоне от 1 до 3600. Значение по умолчанию: 1
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Если устройство часто отправляет запросы ARP, и это влияет на производительность сети, можно установить более длительный интервал повторной передачи запроса ARP. Убедитесь, что этот интервал не превышает тайм-аут ARP

Настройка максимального количества неразрешенных записей ARP

Команда	**arp unresolve** *number*
Описание параметров	*number*: указывает максимальное количество неразрешенных записей ARP в диапазоне от 1 до 8192. Значение по умолчанию: 8192
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Если в таблице кеша ARP существует большое количество неразрешенных записей, которые через некоторое время остаются в таблице, рекомендуется использовать эту команду для ограничения количества неразрешенных записей ARP

2.4.2.5. Пример конфигурации

Сценарий	Топологию сети (Рисунок 2-1)
Этапы конфигурации	• Установите время ожидания ARP на 60 секунд на порте GigabitEthernet 0/1. • Установите интервал повторной передачи запроса ARP на 3 секунд. • Установите время повторной передачи запроса ARP равным 4. • Установите максимальное количество неразрешенных записей ARP равным 4096

	QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#arp timeout 60 QTECH(config-if-GigabitEthernet 0/1)#exit QTECH(config)#arp retry interval 3 QTECH(config)#arp retry times 4 QTECH(config)#arp unresolve 4096
Проверка конфигурации	• Запустите команду **show arp timeout**, чтобы отобразить таймаут интерфейса. • Выполните команду **show running-config**, чтобы отобразить интервал и время повторной передачи запроса ARP, а также максимальное количество неразрешенных записей ARP
	QTECH#show arp timeout Interface arp timeout(sec) ---------- ---------- GigabitEthernet 0/1 60 GigabitEthernet 0/2 3600 GigabitEthernet 0/4 3600 GigabitEthernet 0/5 3600 GigabitEthernet 0/7 3600 VLAN 100 3600 VLAN 111 3600 Mgmt 0 3600 QTECH(config)# show running-config arp unresolve 4096 arp retry times 4 arp retry interval 3

2.4.3. Включение trusted ARP

2.4.3.1. Результат конфигурации

Шлюз защищен от подделки ARP.

2.4.3.2. Этапы конфигурации

Включите trusted ARP в режиме глобальной конфигурации.

2.4.3.3. Проверка конфигурации

Запустите команду **show arp trusted**, чтобы отобразить доверенные записи ARP.

Выполните команду **show running**, чтобы проверить, конфигурацию.

2.4.3.4. Связанные команды

Включение trusted ARP

Команда	**service trustedarp**
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Trusted ARP — это функция защиты от подмены ARP

Включение перенаправления VLAN при добавлении доверенной записи ARP

Команда	**arp trusted user-vlan** *vid1* **translated-vlan** *vid2*
Описание параметров	*vid1*: указывает идентификатор VLAN, настроенный на сервере. *vid2*: указывает идентификатор перенаправленного VLAN
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Эта команда действует только после включения протокола Trusted ARP. Эта команда может быть применена только в том случае, если виртуальная локальная сеть на сервере отличается от виртуальной локальной сети в записи Trusted ARP

Отображение доверенных записей ARP

Команда	**show arp trusted** [*ip* [*mask*]]
Описание параметров	*ip*: указывается IP-адрес. Отображаются записи ARP для указанного IP-адреса. Если указано ключевое слово **trusted**, отображаются только доверенные записи ARP. В противном случае отображаются записи недоверенного ARP. *mask*: отображаются записи ARP в IP-подсети. Если указано ключевое слово **trusted**, отображаются только доверенные записи ARP. В противном случае отображаются записи недоверенного ARP
Режим конфигурации	Привилегированный EXEC режим

Удаление доверенных записей ARP

Команда	**clear arp trusted** [*ip* [*mask*]]
Описание параметров	*ip*: указывается IP-адрес. Отображаются записи ARP указанного IP-адреса. Если указано ключевое слово **trusted**, отображаются только доверенные записи ARP. В противном случае отображаются записи недоверенного ARP. *mask*: отображаются записи ARP в IP-подсети. Если указано ключевое слово **trusted**, отображаются только доверенные записи ARP. В противном случае отображаются записи недоверенного ARP
Режим конфигурации	Привилегированный EXEC-режим
Встроенная подсказка	После выполнения команды **clear arp trusted** для удаления всех доверенных записей ARP на коммутаторе пользователи могут не получить доступ к сети. Рекомендуется использовать команду **clear arp trusted** *ip* для удаления указанной доверенной записи ARP

Включение доверенного устаревания ARP

Команда	**arp trusted aging**
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	После использования этой команды доверенные записи ARP начинают устаревать, с age-time таким же, как для динамического ARP. Для настройки времени устаревания можно запустить команду **arp timeout** в режиме конфигурации интерфейса

Настройка емкости доверенных записей ARP

Команда	**arp trusted** *number*
Описание параметров	*number*: минимальное значение равно 10. Максимальное число — это емкость, поддерживаемая устройством, минус 1024. По умолчанию максимальное количество доверенных записей ARP равно половине общей емкости записей ARP
Режим конфигурации	Привилегированный EXEC-режим

Встроенная подсказка	Чтобы эта команда стала доступна, сначала включите Trusted ARP. Доверенные записи ARP и другие записи совместно используют оперативную память. Если доверенные записи ARP занимают много места, может не остаться места для динамических записей ARP. Задайте количество записей ARP в соответствии с необходимостью. Не задавайте слишком большое значение

2.4.3.5. Пример конфигурации

Сценарий	Топология сети (Рисунок 2-1)
Этапы конфигурации	• Включите Trusted ARP. • Включите перенаправление VLAN. • Включите устаревание Trusted ARP. • Установите максимальное количество записей Trusted ARP равным 1024
	QTECH(config)#service trustedarp QTECH(config)#arp trusted user-vlan 2-9 translated-vlan 10 QTECH(config)#arp trusted aging QTECH(config)#arp trusted 1024
Проверка конфигурации	• Выполните команду **show running-config**, чтобы проверить конфигурацию
	QTECH(config)# show running-config service trustedarp arp trusted user-vlan 2-9 translated-vlan 10 arp trusted aging arp trusted 1024

2.4.3.6. Типичные ошибки

Если trusted ARP отключен, назначения записей ARP невозможно.

2.4.4. Включение Gratuitous ARP

2.4.4.1. Результат конфигурации

Интерфейс периодически отправляет незапрошенные пакеты ARP.

2.4.4.2. Этапы конфигурации

- Опционально.
- Когда коммутатор выступает в качестве шлюза, включите в интерфейсе Gratuitous ARP, чтобы другие пользователи не могли подвергнуться подмене ARP.
- Включите Gratuitous ARP в режиме конфигурации интерфейса.

2.4.4.3. Проверка конфигурации

Запустите команду **show running-config interface** <*name*>, чтобы проверить, успешно ли выполнена конфигурация.

2.4.4.4. Связанные команды

Включение Gratuitous ARP.

Команда	**arp gratuitous-send interval** *seconds* [*number*]
Описание параметров	*seconds*: указывает интервал для отправки Gratuitous ARP запросов. Единица измерения - секунды. Диапазон значений от 1 до 3600. *number*: указывает количество отправленных Gratuitous ARP запросов. Значение по умолчанию: 1. Диапазон значений от 1 до 100
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Если сетевой интерфейс устройства выступает в качестве шлюза для последующих устройств, но устройство, расположенное ниже по потоку, претендует на роль шлюза, включите на интерфейсе Gratuitous ARP, чтобы данное устройство объявило себя настоящим шлюзом

2.4.4.5. Пример конфигурации

Сценарий	Топология сети (Рисунок 2-1)
Этапы конфигурации	Настройте интерфейс GigabitEthernet 0/0 на отправку Gratuitous ARP пакета каждые 5 секунд
	`QTECH(config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5`
Проверка конфигурации	Выполните команду **show running-config interface**, чтобы проверить результат

	QTECH#sh running-config interface gigabitEthernet 0/0 Building configuration... Current configuration : 127 bytes ! interface GigabitEthernet 0/0 duplex auto speed auto ip address 30.1.1.1 255.255.255.0 arp gratuitous-send interval 5

2.4.5. Включение защиты IP-адресов на основе ARP

2.4.5.1. Результат конфигурации

Когда процессор получает указанное количество пакетов, в которых IP-адрес назначения присутствует в записях ARP, все пакеты с этим IP-адресом назначения не будут отправлены на ЦП впоследствии.

2.4.5.2. Этапы конфигурации

- Опционально.
- По умолчанию, установлено значение три неизвестных одноадресных пакета. Пользователи могут выполнить эту команду, чтобы настроить количество пакетов для запуска сброса ARP. Пользователи также могут отключить эту функцию.
- Настройте IP-защиту на основе ARP в режиме глобальной конфигурации.

2.4.5.3. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить результат.

2.4.5.4. Связанные команды

Включение защиты IP-адресов на основе ARP.

Команда	**arp anti-ip-attack** *num*
Описание параметров	*num*: указывает количество IP-пакетов для запуска сброса ARP. Диапазон значений от 0 до 100. 0 указывает на то, что IP-защита на основе ARP отключена. Значение по умолчанию: 3
Режим конфигурации	Режим конфигурации интерфейса

Встроенная подсказка	Если аппаратных ресурсов достаточно, выполните команду arp anti-ipattack num, чтобы установить количество IP-пакетов для запуска сброса ARP на небольшое значение. Если аппаратных ресурсов недостаточно, выполните команду arp anti-ip-attack num, чтобы задать большое количество IP-пакетов для запуска сброса ARP, или отключите эту функцию

2.4.5.5. Пример конфигурации

Сценарий	Топология сети (Рисунок 2-1)
Этапы конфигурации	Включите защиту IP на основе ARP на B. QTECH(config)#arp anti-ip-attack 10
Проверка конфигурации	Выполните команду **show running-config**, чтобы проверить результат
	QTECH#show running-config Building configuration... Current configuration : 53 bytes arp anti-ip-attack 10

2.4.6. Преобразование запросов ARP в запросы аутентификации VLAN

2.4.6.1. Результат конфигурации

Устройство не отправляет пакеты запроса ARP в сети аутентификации VLAN.

2.4.6.2. Примечания

Эта функция поддерживается только на SVI.

2.4.6.3. Этапы конфигурации

- Опционально.
- В режиме аутентификации шлюза устройство по умолчанию не отправляет пакеты запроса ARP в сети аутентификации VLAN. Если устройству необходимо отправить пакеты запроса ARP в сети аутентификации VLAN, выполните команду **no arp suppress-auth-vlan-req**, чтобы отключить эту функцию.
- Выполните эту настройку в режиме конфигурации интерфейса.

2.4.6.4. Проверка конфигурации

Запустите команду **show run interface** <name>, чтобы проверить результат.

2.4.6.5. Связанные команды

Преобразование запросов ARP в запросы аутентификации VLAN.

Команда	**arp suppress-auth-vlan-req**
Режим конфигурации	Режим конфигурации интерфейса

2.4.6.6. Пример конфигурации

Сценарий	Топология сети (Рисунок 2-1)
Этапы конфигурации	Отключите интерфейс VLAN 2 от передачи запросов ARP в сети аутентификации VLAN. QTECH(config-if-VLAN 2)#no arp suppress-auth-vlan-req
Проверка конфигурации	Запустите команду **show running-config interface** *<name>*, чтобы проверить результат
	QTECH#show running-config interface vlan 2 Building configuration... Current configuration : 53 bytes interface VLAN 2 ip address 192.168.1.2 255.255.255.0 no arp suppress-auth-vlan-req

2.5. Контроль состояния

2.5.1. Очистка

Выполнение команд **clear** может привести к потере важной информации и, следовательно, прерыванию работы служб.

Описание	**Команда**
Очищает динамические ARP-записи. В режиме аутентификации шлюза динамические записи ARP в сетях аутентификации VLAN не очищаются	**clear arp-cache**

2.5.2. Отображение

Описание	Команда
Отображает таблицу ARP в подробном виде	**show arp** [**detail**] **[** *interface-type interface-number* | [**vrf** *vrfname*] [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete]**
Отображает таблицу ARP	**show ip arp [vrf** *vrf-name* **]**
Отображает таблицу доверенных ARP	**show arp** [**detail**] **trusted** [*ip* [*mask*]]
Отображает счетчик записей ARP	**show arp counter**
Отображает таймаут динамических записей ARP	**show arp timeout**

2.5.3. Отладка

Системные ресурсы используются для вывода отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Включает отладку отправки и получения пакетов ARP	**debug arp**
Включает отладку создания и удаления записей ARP	**debug arp event**

3. НАСТРОЙКА IPV6

3.1. Обзор

По мере быстрого развития Интернета и исчерпания адресного пространства IPv4, ограничения IPv4 становятся все более очевидными. В настоящее время проведено множество исследований и практик по интернет-протоколу следующего поколения (IPng). Рабочая группа IPng в составе группы разработчиков по проектированию Интернета (IETF) разработала протокол IPng с именем IP версии 6 (IPv6), который описан в RFC 2460.

3.1.1. Основные функции

Больше адресное пространство

По сравнению с 32-битным адресом IPv4 длина адреса IPv6 увеличивается до 128 бит. Таким образом, адресное пространство имеет около 2^{128} адресов. IPv6 использует иерархический режим распределения адресов для поддержки назначения адресов нескольких подсетей из основной сети Интернет в подсеть интрасети.

Упрощенный формат заголовка пакета

Поскольку принцип проектирования заголовка пакета IPv6 заключается в минимизации издержек заголовка пакета, некоторые неключевые поля и дополнительные поля удаляются из заголовка пакета в расширенный заголовок пакета. Поэтому, хотя длина IPv6-адреса в четыре раза превышает длину IPv4адреса, заголовок пакета IPv6 всего вдвое больше заголовка пакета IPv4. Заголовок пакета IPv6 делает пересылку на устройствах более эффективной. Например, при отсутствии контрольной суммы в заголовке пакета IPv6 устройству IPv6 не нужно обрабатывать фрагменты (фрагментация выполняется инициатором).

Эффективная иерархическая адресация и структура маршрутизации

IPv6 использует механизм конвергенции и определяет гибкую иерархическую адресацию и структуру маршрутизации. Несколько сетей на одном уровне представлены в виде единого сетевого префикса на восходящем устройстве, что значительно сокращает количество записей маршрутизации, обслуживаемых устройством, а также накладные расходы на маршрутизацию и хранение устройства.

Простота управления: Plug and Play (PnP)

Протокол IPv6 предоставляет функции автоматического обнаружения и автоматической настройки для упрощения управления и обслуживания сетевых узлов. Например, обнаружение соседей (ND), обнаружение MTU, объявления маршрутизатора (RA), запросы маршрутизатора (RS) и технологии автоматической настройки предоставляют сопутствующие услуги для PnP. В частности, IPv6 предлагает два типа автоматической настройки: автонастройка с сохранением состояния и автонастройка без сохранения состояния. В IPv4 протокол динамической конфигурации хоста (DHCP) выполняет автоматическую настройку IP-адреса хоста и связанных с ним параметров. IPv6 наследует эту службу автоматической настройки из IPv4 и называет ее автонастройкой с отслеживанием состояния (см. DHCPv6). Кроме того, IPv6 также предлагает услугу автоматической настройки без сохранения состояния. При автоматической настройке без сохранения состояния хост автоматически получает локальный адрес канала, префикс адреса локального устройства и другие связанные конфигурации.

Безопасность

В качестве дополнительного протокола расширения IPv4 протокол IPSec (Internet Protocol Security) является частью протокола IPv6 для обеспечения безопасности пакетов IPv6. В настоящее время протокол IPv6 содержит два механизма: Заголовок аутентификации

(Authentication Header, AH) и инкапсулированная полезная нагрузка системы безопасности (Encapsulated Security Payload, ESP). Заголовок аутентификации обеспечивает целостность данных и аутентифицирует IP источников пакетов, чтобы гарантировать, что пакеты происходят от узлов, определенных адресами источника. ESP обеспечивает шифрование данных для реализации сквозного шифрования.

Улучшенная поддержка QoS

Новое поле в заголовке пакета IPv6 определяет способ идентификации и обработки потоков данных. Поле Flow Label в заголовке пакета IPv6 используется для аутентификации потока данных. Используя это поле, IPv6 позволяет пользователям предлагать требования к качеству связи. Устройство может идентифицировать все пакеты, принадлежащие определенному потоку данных, на основе этого поля и обрабатывать эти пакеты в соответствии с требованиями пользователя.

Новый протокол для взаимодействия с соседним узлом

Протокол обнаружения соседних узлов IPv6 (NDP) использует серию пакетов протокола сообщений управления Интернетом версии 6 (ICMPv6) для реализации интерактивного управления соседними узлами (узлами по одному каналу). IPv6 использует NDP-пакеты и эффективные ND-пакеты многоадресной/одноадресной рассылки вместо пакетов обнаружения маршрутизатора с протоколом разрешения адресов на основе широковещательной рассылки (ARP) и протоколом управления сообщениями версии 4 (ICMPv4).

Расширяемость

Благодаря высокой расширяемости функции IPv6 могут быть добавлены в расширенный заголовок пакета после заголовка пакета IPv6. В отличие от IPv4, заголовок пакета IPv6 может поддерживать более 40 байт параметров. Для пакета IPv6 длина расширенного заголовка пакета ограничена только максимальным количеством байт в пакете.

3.1.1.1. Протоколы и стандарты

- RFC 4291 — архитектура адресации IP версии 6.
- RFC 2460 — спецификация интернет-протокола, версия 6 (IPv6).
- RFC 4443 — протокол ICMPv6 для протокола Интернета версии 6 (IPv6).
- RFC 4861 — обнаружение соседей для IP версии 6 (IPv6).
- RFC 4862 — автоматическая настройка IPv6-адреса без сохранения состояния.
- RFC 5059 — исключение заголовков маршрутизации типа 0 в IPv6.

3.2. Применение

Применение	Описание
Связь на основе адресов IPv6	Два ПК обмениваются данными друг с другом с помощью адресов IPv6

3.2.1. Связь на основе адресов IPv6

3.2.1.1. Сценарий

Как показано на Рисунке 3-1, узел 1 и узел 2 обмениваются данными друг с другом с помощью адресов IPv6.

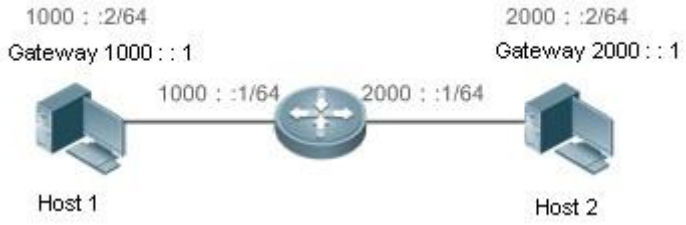


Рисунок 3-1.

3.2.1.2. Описание

Хосты могут использовать режим автоматической настройки адреса без сохранения состояния или назначение адреса по DHCPv6. После настройки адресов узлы могут обмениваться данными друг с другом с помощью адресов IPv6.

3.3. Ключевые особенности

3.3.1. Обзор

Функция	Описание
Формат адреса IPv6	Формат IPv6-адреса делает IPv6 более крупным адресным пространством и более гибким представительским подходом
Тип адреса IPv6	IPv6 определяет сетевые приложения на основе адресов
Формат заголовка пакета IPv6	IPv6 упрощает фиксированные и расширенные заголовки пакетов для повышения эффективности обработки и пересылки пакетов данных устройства
IPv6 PMTUD (Path MTU Discovery)	Хост динамически обнаруживает и настраивает размер MTU на пути передачи данных, экономя ресурсы маршрутизатора и повышая эффективность сети IPv6
Обнаружение соседей IPv6	Функции ND включают обнаружение маршрутизатора, обнаружение префиксов, обнаружение параметров, автонастройку адреса, разрешение адреса (например, ARP), определение следующего перехода, обнаружение недоступности соседнего узла (NUD), обнаружение дублирующихся адресов (DAD) и перенаправление
Маршрут источника IPv6 (IPv6 Source Routing)	Эта функция используется для указания промежуточных узлов, через которые пакет проходит по пути к адресу назначения. Это аналогично опциям IPv4 loose source routing и loose record routing

Функция	Описание
Ограничение скорости отправки сообщений об ошибках ICMPv6	Эта функция предотвращает DoS-атаки
Ограничение перехода IPv6	Эта функция предотвращает бесполезную одноадресную передачу пакетов по сети и потерю пропускной способности сети
Преобразование из отправки пакетов NS в сети аутентификации VLAN	В режиме аутентификации шлюза устройство не передает пакеты NS в сети аутентификации VLAN
Шлюз по умолчанию в интерфейсе управления	Шлюз по умолчанию настроен в интерфейсе управления для создания маршрута по умолчанию для этого интерфейса

3.3.2. Формат адреса IPv6

Адрес IPv6 представлен в формате X:X:X:X:X:X:X:X:X, где X — это 4-значное шестнадцатеричное число (16 бит). Каждый адрес состоит из 8 целых чисел, всего 128 бит (каждое целое число содержит 4 шестнадцатеричных цифры, а каждая цифра содержит четыре бита). Ниже приведены три допустимых адреса IPv6:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

Эти целые числа являются шестнадцатеричными, где от A до F обозначает от 10 до 15. Каждое целое число в адресе должно быть представлено, за исключением нулей в начале каждого целого числа. Если IPv6-адрес содержит строку нулей (как показано на втором и третьем примерах выше), то для отображения этих нулей можно использовать двойное двоеточие (::). То есть, 800:0:0:0:0:0:0:1 можно представить как 800::1.

Двоеточие означает, что этот адрес может быть расширен до полного 128-битного адреса. При таком подходе, только если 16-битные целые числа имеют все 0, их можно заменить двойным двоеточием. Двойное двоеточие может использоваться в IPv6-адресе только единожды.

В смешанной среде IPv4/IPv6 адрес имеет смешанное представление. В адресе IPv6 для представления IPv4-адреса можно использовать младшие 32 бита. Этот адрес IPv6 может быть представлен в смешанном виде, то есть X:X:X:X:X:X:d.d.d.d, где X — это шестнадцатеричное целое число, а d — 8-разрядное десятичное число. Например, 0:0:0:0:0:0:192.168.20.1 является допустимым адресом IPv6. Его можно сократить до :::192.168.20.1. Типичными приложениями являются адреса IPv6, совместимые с IPv4, и адреса IPv6, привязанные к IPv4. Если первые 96-бит имеют адрес 0 в IPv4-совместимом IPv6-адресе, этот адрес может быть представлен как ::A.B.C.D, например ::1.1.1.1. В настоящее время адреса, совместимые с IPv4, отменены. Адреса IPv6, привязанные к IPv4, представлены как ::FFFF:A.B.C.D для представления адресов IPv4 в качестве адресов IPv6. Например, адрес IPv4 1.1.1.1, сопоставленный с адресом IPv6, представляется как ::FFFF:1.1.1.1.

Поскольку IPv6-адрес разделен на две части: префикс подсети и идентификатор интерфейса, он может быть представлен в виде адреса с дополнительным значением в соответствии с методом выделения адресов, таким как бесклассовая междоменная маршрутизация (CIDR). Дополнительное значение указывает, сколько битов (префикса подсети) в адресе соответствует сетевой части. То есть, адрес узла IPv6 содержит длину префикса. Длина префикса отделена от адреса IPv6 косой чертой. Например, в 12AB::CD30:0:0:0:0/60 длина префикса, используемого для маршрутизации, составляет 60 бит.

3.3.2.1. Связанная конфигурация

Настройка IPv6-адреса.

- По умолчанию в интерфейсах не настроен IPv6-адрес.
- Выполните команду **ipv6 address**, чтобы настроить IPv6-адрес на интерфейсе.
- После настройки хост может обмениваться данными с другими пользователями, используя настроенный IPv6-адрес на основе DAD.

3.3.3. Тип адреса IPv6

RFC 4291 определяет три типа адресов IPv6:

- Одноадресный (Unicast) адрес: идентификатор одного интерфейса. Пакеты, предназначенные для одноадресного адреса, отправляются в интерфейс, указанный по этому адресу.
- Адрес многоадресной рассылки (Multicast): идентификатор группы интерфейсов (интерфейсы обычно принадлежат разным узлам). Пакеты, предназначенные для многоадресного адреса, отправляются на все интерфейсы, включенные в этот адрес.
- Адрес Anycast: идентификатор группы интерфейса. Пакеты, предназначенные для адреса в любом случае, отправляются на один интерфейс, включенный в этот адрес (ближайший интерфейс в соответствии с протоколом маршрутизации).

ПРИМЕЧАНИЕ: IPv6 не определяет адреса широковещательной рассылки.

Эти три типа адресов описаны следующим образом:

- Unicast-адреса

Unicast-адреса делятся на пять типов: unspecified адрес, loopback адрес, link-local адрес, site-local адрес, and global unicast-адрес. В настоящее время site-local-адрес отменен. За исключением unspecified, loopback и link-local, все остальные адреса являются глобальными unicast-адресами.

- Unspecified (неопределенный) адрес

Unspecified адрес **0:0:0:0:0:0:0:0**, который обычно сокращен до **::**. Он имеет две общие цели:

1. Если при запуске узла не указан unicast-адрес, он использует неопределенный адрес в качестве исходного адреса для отправки пакета RS для получения префиксной информации от шлюза и, таким образом, генерации unicast-адреса.
2. Если для хоста настроен IPv6-адрес, устройство определяет, конфликтует ли адрес с адресами других хостов в том же сегменте сети и использует неопределенный адрес в качестве исходного адреса для отправки пакета запроса соседей (NS) (аналогично ARP-пакету).

- Loopback-адрес

Адрес обратной связи **0:0:0:0:0:0:0:1**, который обычно сокращен до **::1**. Подобно IPv4-адресу **127.0.0.1**, Loopback-адрес обычно используется узлом для отправки пакетов.

- Link-local адрес

Формат локального адреса канала:

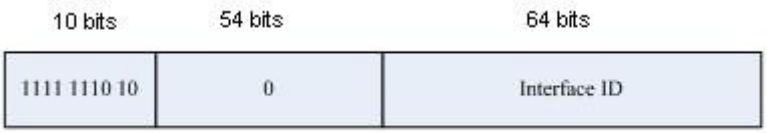


Рисунок 3-2.

Локальный адрес канала используется в одном сетевом канале для назначения идентификаторов хостам. Адрес, идентифицируется первыми 10 битами в префиксе, является локальным адресом канала. Устройство никогда не пересылает пакеты, в которых адрес источника или назначения содержит локальный адрес канала. Промежуточные 54 бита в адресе являются 0. Последние 64 бита представляют идентификатор интерфейса, который позволяет одной сети подключать 2^{64}-1 узлов.

- Site-local адрес

Формат site-local адреса:

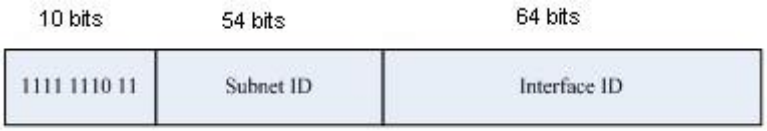


Рисунок 3-3.

Site-local адрес используется для передачи данных в пределах сети. Устройство никогда не пересылает пакеты, в которых адрес источника или назначения содержит site-local. То есть, эти пакеты могут быть переадресованы только внутри LAN. Такие адреса аналогичны частным адресам IPv4, таким как 192.168.0.0/16. RFC 3879 отменил site-local адреса. Новые адреса не поддерживают первые 10 бит в качестве префикса и считаются глобальными одноадресными адресами. Существующие адреса могут продолжать использовать этот префикс.

- Глобальный unicast адрес

Формат глобального unicast адреса:

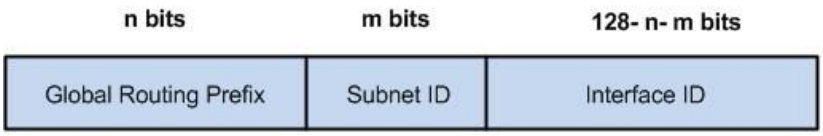


Рисунок 3-4.

Среди глобальных unicast адресов существует тип IPv4-встроенных адресов IPv6, включая IPv4-совместимые адреса IPv6 и IPv4-сопоставленные адреса IPv6. Они используются для соединения между узлами IPv4 и узлами IPv6.

Формат IPv6-адреса, совместимого с IPv4, следующий:

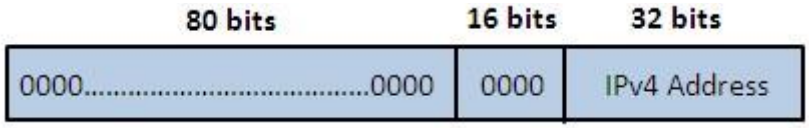


Рисунок 3-5.

Формат IPv6-адреса, сопоставленного с IPv4, следующий:

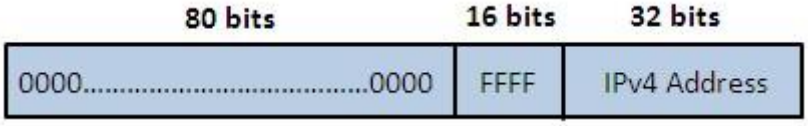


Рисунок 3-6.

IPv6-адреса, совместимые с IPv4, в основном используются в автоматических туннелях. Узлы в автоматических туннелях поддерживают как IPv4, так и IPv6. Используя эти адреса, устройства IPv4 передают пакеты IPv6 через туннели. В настоящее время адреса IPv6, совместимые с IPv4, отменены. IPv6-адреса, сопоставленные с IPv4, используются узлами IPv6 для доступа к только IPv4 узлам. Например, если приложение IPv6 на хосте IPv4/IPv6 запрашивает разрешение на имя хоста только для IPv4, сервер имен динамически генерирует адрес IPv6, привязанный к IPv4, и возвращает его приложению IPv6.

- Адреса multicast

Формат multicast-адреса IPv6:

```
|  8    | 4 | 4 |        112 bits             |
+--------+----+----+-----------------------------------------+
|11111111|flgs|scop|        group ID             |
+--------+----+----+-----------------------------------------+
```

Первый байт в адресе — все единицы, представляющие адрес multicast.

- Поле флага

Поле флага состоит из четырех битов. В настоящее время указывается только четвертый бит, указывающий, является ли этот адрес известным адресом multicast рассылки, назначенным органом IANA (Internet Assigned Numbers Authority), или временным адресом многоадресной рассылки в определенном сценарии. Если флаг имеет значение 0, этот адрес является известным адресом multicast. Если флаг имеет значение 1, этот адрес является временным адресом multicast рассылки. Остальные три флага зарезервированы для использования в будущем.

- Области

Поле SCOPE состоит из четырех битов, указывающих диапазон multicast передачи. То есть, группа multicast рассылки включает локальный узел, локальный канал, локальный узел и любой узел в глобальной адресной области IPv6.

- Поле идентификатора группы

Идентификатор группы состоит из 112 бит для идентификации группы multicast рассылки. Идентификатор multicast рассылки может представлять различные группы на основе полей флага и области действия.

Адреса многоадресной рассылки IPv6 имеют префикс FF00::/8. Один адрес многоадресной рассылки IPv6 обычно идентифицирует интерфейсы на нескольких разных узлах. После отправки пакета на адрес multicast рассылки пакет пересылается на интерфейсы каждого

узла, указанного по этому адресу multicast рассылки. Для узла (хоста или устройства) необходимо добавить следующие адреса multicast рассылки:

1. multicast адрес для всех узлов локального канала, то есть FF02::1.
2. Адрес multicast рассылки узла, предварительно исправленный с FF02:0:0:0:0:1:FF00:0000/104.

Если узел является устройством, он также должен быть добавлен к multicast адресам всех устройств в локальном канале, то есть, FF02::2.

Адрес multicast рассылки для запрашиваемых узлов соответствует адресу unicast. Необходимо добавить соответствующий адрес multicast рассылки для каждого настроенного адреса unicast. Адрес multicast рассылки для запрашиваемых узлов префикса FF02:0:0:0:0:1:FF00:0000/104. Остальные 24 бит состоят из наименее значимых 24 бит unicast. Например, если адрес unicast рассылки FE80::2AA:FF:FE21:1234, адрес multicast рассылки запрашиваемых узлов FF02::1:FF21:1234.

Адрес multicast рассылки для запрашиваемых узлов обычно используется в пакетах NS. Формат адреса:

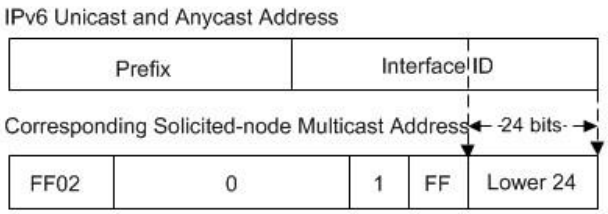


Рисунок 3-7.

Адреса anycast

Подобно многоадресным адресам, адрес anycast также может совместно использоваться несколькими узлами. Разница заключается в том, что только один узел в адресе anycast получает пакеты данных, а все узлы, включенные в адрес многоадресной рассылки, получают пакеты данных. Поскольку адреса в любом формате выделяются для обычного одноадресного пространства IPv6, они имеют одинаковые форматы с одноадресными адресами. Каждый участник в любом адресе должен быть настроен явным образом для облегчения распознавания. Адреса Anycast могут быть назначены только устройствам и не могут использоваться в качестве адресов источника пакетов.

RFC 2373 переопределяет адрес в любом случае, называемый адресом подсети маршрутизатора. Рисунок 3-8 показывает формат адреса anycast-router. Такой адрес состоит из префикса подсети и серии 0 (ИД интерфейса).

Префикс подсети определяет указанную ссылку (подсеть). Пакеты, предназначенные для адреса anycast маршрутизатора подсети, будут пересылаться на устройство в этой подсети. Адрес anycast маршрутизатора обычно используется приложением на узле для связи с устройством в удаленной подсети.

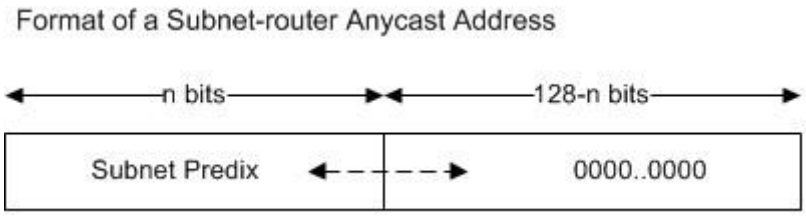


Рисунок 3-8.

3.3.3.1. Связанная конфигурация

Настройка IPv6-адреса.

- По умолчанию в интерфейсах не настроен IPv6-адрес.
- Выполните команду **ipv6 address**, чтобы настроить unicast адрес IPv6 и адрес интерфейса в любом случае.
- После того, как интерфейс включится, он автоматически присоединится к соответствующей группе multicast.

3.3.4. Формат заголовка пакета IPv6

Рисунок 3-9 показывает формат заголовка пакета IPv6.

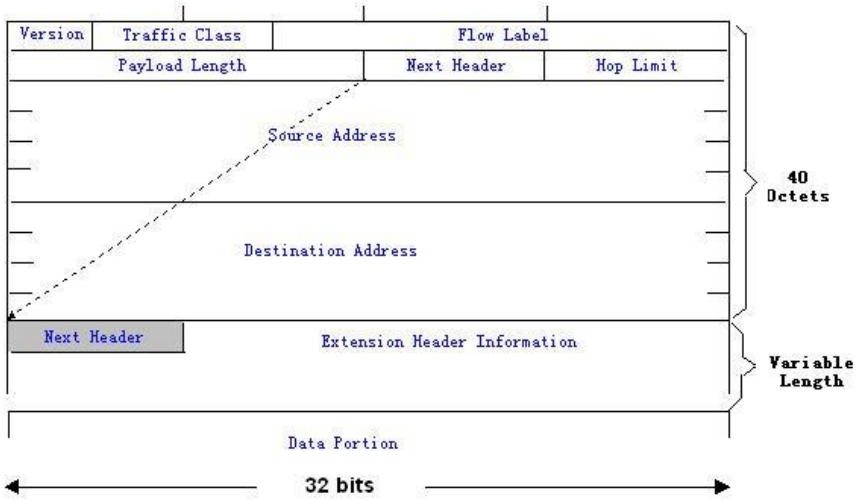


Рисунок 3-9.

Заголовок пакета IPv4 состоит из четырех байт. Заголовок пакета IPv6 состоит из 40 байт объединенных по восемь байт. Заголовок пакета IPv6 содержит следующие поля:

- Версия

Это поле состоит из 4 бит. В адресе IPv6 это поле должно быть 6.

- Класс трафика

Это поле состоит из 8 бит. В этом поле указывается служба, предоставляемая этим пакетом, как и в поле TOS в адресе IPv4.

- Метка потока

Это поле состоит из 20 бит для идентификации пакетов, принадлежащих одному и тому же потоку услуг. Один узел может выступать в качестве источника передачи для нескольких потоков обслуживания. Метка потока и адрес источника однозначно идентифицируют один поток обслуживания.

- Длина полезной нагрузки

Это поле состоит из 16 бит, включая длину полезной нагрузки пакета и длину расширенных параметров IPv6 (если доступно). То есть, он включает длину пакета IPv6, кроме заголовка пакета IPv6.

- Следующий заголовок

В этом поле указывается тип протокола в поле заголовка после заголовка пакета IPv6. Как и в поле Protocol (Протокол) в заголовке IPv4-адреса, поле Next Header (Следующий

заголовок) используется для указания того, использует ли верхний слой протокол TCP или UDP. Он также может использоваться для указания наличия заголовка расширения IPv6.

- Ограничение переходов (Hop Limit)

Это поле состоит из 8 бит. При каждой пересылаемой устройством пакетной передаче значение поля уменьшается на 1. Если значение поля достигает 0, этот пакет будет удален. Это похоже на поле Lifetime в заголовке пакета IPv4.

- Адрес источника

Это поле состоит из 128 бит и указывает адрес отправителя в пакете IPv6.

- Адрес назначения

Это поле состоит из 128 бит и указывает адрес получателя в пакете IPv6.

В настоящее время IPv6 определяет следующие заголовки расширений:

- Параметры перехода (Hop-By-Hop)

Этот заголовок расширения должен следовать за заголовком пакета IPv6. Он состоит из данных параметров, которые необходимо проверить на каждом узле по пути.

- Параметры маршрутизации (заголовок маршрутизации типа 0)

Этот заголовок внутреннего номера указывает узлы, через которые пакет проходит от исходного адреса до адреса назначения. Он состоит из адресного списка узлов passerby. Начальный адрес назначения в заголовке пакета IPv6 — это первый адрес среди адресов в заголовке маршрутизации, но не конечный адрес назначения пакета. После того, как узел, соответствующий адресу назначения в заголовке пакета IPv6, получает пакет, он обрабатывает заголовок пакета IPv6 и заголовок маршрутизации и отправляет пакет на второй адрес, третий адрес, и так далее в списке заголовков маршрутизации до тех пор, пока пакет не достигнет конечного адреса назначения.

- Фрагмент

Исходный узел использует этот заголовок расширения для фрагментации пакетов, длина которых превышает MTU пути (PMTU).

- Параметры назначения

Этот заголовок расширения заменяет поля параметров IPv4. В настоящее время поле параметры назначения может быть заполнено только целым числом, кратным 64 бит (восемь байт), если это необходимо. Этот заголовок внутреннего номера может использоваться для передачи информации, которую будет проверять узел назначения.

- Верхний слой заголовка

Этот заголовок расширения указывает на протокол, используемый на верхнем уровне, например, TCP (6) и UDP (17).

Еще два заголовка расширения AH и ESP будут описаны в разделе *Настройка IPSec*.

3.3.5. IPv6 PMTUD (Path MTU Discovery)

Подобно обнаружению MTU пути IPv4 (PMTUD), IPv6 PMTUD позволяет хосту динамически обнаруживать и регулировать размер MTU на пути передачи данных. Если длина пакета данных, который должен быть отправлен хостом, превышает PMTU, узел самостоятельно выполняет фрагментацию пакетов. Таким образом, устройству IPv6 не нужно выполнять фрагментацию, экономить ресурсы устройств и повышать эффективность сети IPv6.

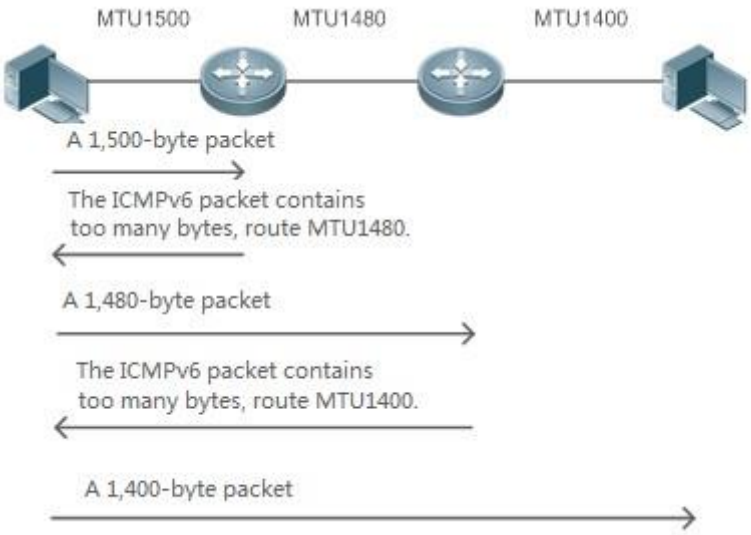


Рисунок 3-10.

Как показано на Рисунке 3-10, если длина пакета, который должен быть отправлен хостом, превышает MTU, маршрутизатор отбрасывает этот пакет и отправляет на хост сообщение ICMPv6 Packet Too Big, содержащее PMTU. После этого хост фрагментирует пакет на основе нового PMTU. Таким образом, маршрутизатору не нужно выполнять фрагментацию, это экономит ресурсы маршрутизатора и повышать эффективность сети IPv6.

3.3.5.1. Связанная конфигурация

Настройка MTU IPv6 интерфейса

- По умолчанию MTU IPv6 составляет 1500 на интерфейсе Ethernet.
- Чтобы уменьшить трафик, вызванный отбраковкой пакетов, необходимо установить правильное значение MTU в соответствии с фактической сетевой средой. Выполните команду **ipv6 mtu**, чтобы изменить MTU IPv6-интерфейса.

3.3.6. Обнаружение соседей IPv6

Протокол NDP является основной частью протокола IPv6. Его основные функции включают обнаружение маршрутизатора, обнаружение префиксов, обнаружение параметров, автонастройку адреса, разрешение адреса (например, ARP), определение следующего перехода, NUD, DAD и перенаправление. NDP определяет пять пакетов ICMP: RS (тип ICMP: 133), RA (тип ICMP: 134), NS (аналогично запросу ARP, тип ICMP: 135), NA (аналогично ответу ARP, типу ICMP: 136), ICMP Redirect (тип ICMP: 137).

Все вышеперечисленные пакеты ICMP имеют одну или несколько опций. В некоторых случаях эти опции являются необязательными, но в других случаях они являются существенными. В основном NDP определяет пять опций: Параметр адреса исходного уровня связи, Type=1; параметр адреса целевого уровня связи, Type=2; параметр информации префикса, Type=3; параметр заголовка перенаправления, Type=4; MTU Option, Type=5.

Разрешение адресов

Когда узел пытается установить связь с другим узлом, узел должен получить адрес 2 уровня узла, отправив ему пакет NS. В этом пакете адресом назначения является адрес многоадресной рассылки узла, соответствующий IPv6-адресу узла назначения. Этот пакет также содержит адрес уровня канала исходного узла. После получения этого пакета NS

концевой узел получает ответный пакет NA, в котором адресом назначения является исходный адрес пакета NS, то есть адрес уровня канала запрашиваемого узла. После получения этого пакета NA исходный узел может обмениваться данными с узлом назначения.

Рисунок 3-11 показывает процесс разрешения адресов.

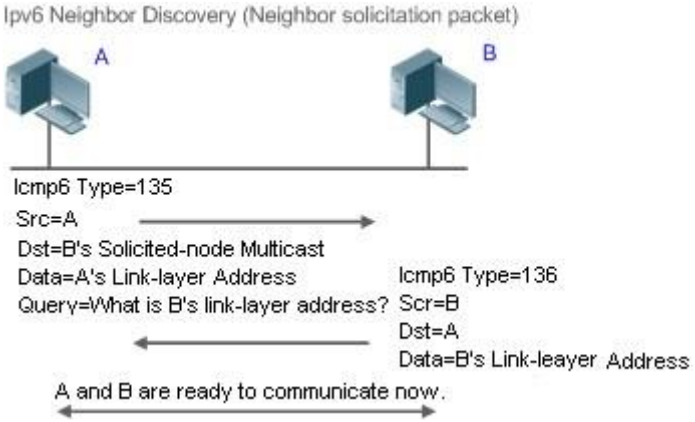


Рисунок 3-11.

NUD

Если время доступности соседа истекло, но требуется отправить unicast пакет IPv6, устройство выполняет NUD.

При выполнении NUD устройство может продолжать пересылать пакеты IPv6 соседу.

DAD

Чтобы узнать, уникален ли адрес IPv6, настроенный для хоста, устройство должно выполнить DAD, отправив пакет NS, в котором исходный адрес IPv6 является неопределенным.

Если устройство обнаруживает конфликт адресов, для этого адреса устанавливается состояние дублирования, чтобы устройство не получало пакеты IPv6 с таким адресом назначения. В то же время устройство также запускает таймер для этого дублирующего адреса, чтобы периодически выполнять DAD. Если при повторном обнаружении конфликта адресов не обнаружено, этот адрес можно использовать.

Маршрутизатор, Префикс и Обнаружение параметров

Устройство периодически отправляет пакеты RA всем локальным узлам канала.

Рисунок 3-12 показывает процесс отправки пакета RA.

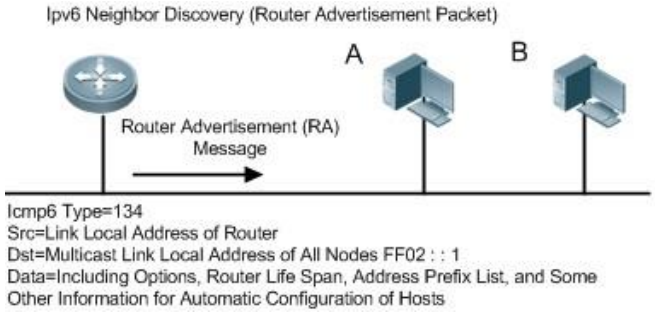


Рисунок 3-12.

Пакет RA обычно содержит следующее содержимое:

- Один или несколько префиксов IPv6-адресов (используется для определения по каналу или автоматической настройки адреса без сохранения состояния).
- Действительность префикса адреса IPv6.
- Метод автоматической настройки хоста (с сохранением состояния или без сохранения состояния).
- Информация об устройстве по умолчанию (независимо от того, работает ли устройство по умолчанию; если да, то также включается интервал для действий в качестве устройства по умолчанию).
- Другая информация, предоставляемая для конфигурации хоста, например, ограничение переходов, MTU и интервал повторной передачи NS.

Пакеты RA также могут использоваться в качестве ответов на пакеты RS, отправленные хостом. С помощью пакетов RS хост может получить автоматически настроенную информацию сразу после запуска, а не ждать, пока RA-пакеты будут отправлены устройством. Если для вновь запущенного хоста не настроен unicast адрес, то в качестве исходного адреса в пакете RS хост включает неопределенный адрес (0:0:0:0:0:0:0:0). В противном случае хост использует настроенный unicast адрес в качестве исходного и multicast адреса всех локальных устройств маршрутизации (FF02::2) в качестве адреса назначения в пакете RS. В качестве ответа на пакет RS пакет RA использует адрес источника пакета RS в качестве адреса назначения (если адрес источника не указан, он использует адрес многоадресной рассылки всех локальных узлов (FF02::1).

В пакете RA можно настроить следующие параметры:

- RA-интервал: интервал отправки пакета RA.
- RA-срок службы: срок службы маршрутизатора, то есть, действует ли устройство в качестве маршрутизатора по умолчанию на локальном канале, а также интервал выполнения функций маршрутизатора по умолчанию.
- Префикс: префикс адреса IPv6 в локальной ссылке. Он используется для автоматического определения адреса в режиме on-link или автоматической настройки адреса без сохранения состояния, включая другие конфигурации параметров, связанные с префиксом.
- Интервал NS: интервал повторной передачи пакетов NS.
- Время ожидания: период, когда устройство рассматривает соседний узел, доступного после обнаружения события подтверждения доступности соседнего узла.
- RA-hoplimit: лимит пакета RA, используемый для установки ограничения перехода хоста для отправки одноадресного пакета.
- RA-mtu: MTU пакета RA.
- Managed-config-flag: получает ли хост этот пакет RA адрес через автонастройку с отслеживанием состояния.
- Other-config-flag: использует ли хост, получающий этот пакет RA DHCPv6 для получения другой информации, кроме IPv6-адреса для автоматической настройки.

Настройте указанные выше параметры при настройке атрибутов интерфейса IPv6.

Перенаправление

Если маршрутизатор, получающий пакет IPv6, находит более эффективный следующий переход (next hop), он отправляет пакет ICMP Redirect, чтобы сообщить узлу о более удачных последующих переходах. Хост будет напрямую отправлять пакет IPv6 в следующий раз на более лучший переход.

Максимальное количество неразрешенных записей ND

- Можно настроить максимальное количество неразрешенных записей ND, чтобы предотвратить создание неразрешенных записей ND в сетевых сегментах злоумышленником, занимающим избыточное пространство памяти.

Максимальное количество записей обучения соседей в интерфейсе

- Вы можете настроить максимальное количество записей обучения соседей на интерфейсе, чтобы предотвратить попадание атак соседних узлов на ND записи и пространство памяти устройства и повлиять на эффективность пересылки устройства.

3.3.6.1. Связанная конфигурация

Включение перенаправления IPv6

- По умолчанию пакеты перенаправления ICMPv6 могут быть отправлены на интерфейсы IPv6.
- Выполните команду **no ipv6 redirects** в режиме конфигурации интерфейса, чтобы запретить интерфейсу отправлять пакеты Redirect.

Настройка IPv6 DAD

- По умолчанию интерфейс отправляет один пакет NS для выполнения IPv6 DAD.
- Запустите команду **ipv6 nd dad attempts** *value* в режиме конфигурации интерфейса, чтобы настроить количество пакетов NS, последовательно отправленных DAD. Значение 0 указывает на отключение DAD для адресов IPv6 на этом интерфейсе.
- Выполните команду **no ipv6 nd dad attempts**, чтобы восстановить конфигурацию по умолчанию.
- По умолчанию устройство выполняет DAD по дублирующимся адресам IPv6 каждые 60 секунд.
- Выполните команду **ipv6 nd dad retry** *value* в режиме глобальной конфигурации, чтобы настроить интервал DAD. Значение 0 указывает на отключение DAD для устройства.
- Выполните команду **no ipv6 nd dad retry**, чтобы восстановить конфигурацию по умолчанию.

Настройка доступного времени соседнего узла

- По умолчанию для соседнего узла IPv6 установлено значение 30 секунд.
- Выполните команду **ipv6 nd reachable-time** *milliseconds* в режиме конфигурации интерфейса, чтобы изменить время, в течение которого можно достичь соседа.

Настройка времени устаревшей конфигурации соседа

- По умолчанию время устаревания конфигурации для соседнего узла IPv6 установлено 1 час. По истечении этого времени устройство выполняет NUD.
- Запустите команду **ipv6 nd stale-time** *seconds* в режиме конфигурации интерфейса, чтобы изменить время устаревания соседа. Настройка информации префикса
- По умолчанию префикс в пакете RA на интерфейсе — это префикс, настроенный в команде **ipv6 address** интерфейса.
- Выполните команду **ipv6 nd prefix** в режиме конфигурации интерфейса, чтобы добавить или удалить префиксы и параметры префиксов, которые могут быть объявлены.

Включение/отключение подавления RA

- По умолчанию интерфейс IPv6 не отправляет пакеты RA.
- Запустите команду **no ipv6 nd suppress-ra** в режиме конфигурации интерфейса, чтобы отключить подавление RA.

Настройка максимального количества неразрешенных записей ND

- Значение по умолчанию 0, указывающее на отсутствие ограничений. Она ограничена только пропускной способностью ввода ND, поддерживаемой устройством.
- Запустите команду **ipv6 nd unresolved** *number* в режиме глобальной конфигурации, чтобы ограничить число неразрешенных соседей. После того как записи превысят это ограничение, устройство не будет активно разрешать последующие пакеты.

Настройка максимального количества записей ND, полученных в интерфейсе

- Запустите команду **ipv6 nd cache interface-limit** *value* в режиме конфигурации интерфейса, чтобы ограничить количество соседей, которые узнали на интерфейсе. Значение по умолчанию 0, указывающее на отсутствие ограничений.

3.3.7. Маршрут источника IPv6 (IPv6 Source Routing)

3.3.7.1. Принцип работы

Аналогично опциям source route, loose source route, и record route IPv4, заголовок IPv6 используется для указания промежуточных узлов, через которые пакет проходит по пути к адресу назначения. Он использует следующий формат:

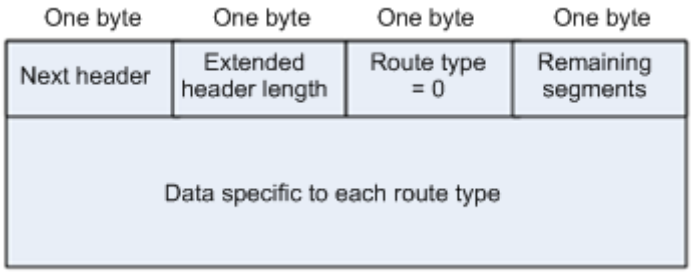


Рисунок 3-13.

Поле Segments Left используется для указания количества промежуточных узлов, указанных в заголовке маршрутизации пакета, который должен пройти от текущего узла до конечного адреса назначения.

В настоящее время определены два типа маршрутизации: 0 и 2. Заголовок маршрутизации Type 2 используется для мобильной связи. RFC 2460 определяет заголовок маршрутизации Type 0 (аналогично опции маршрутизации свободного источника IPv4). Формат заголовка маршрутизации Type 0:

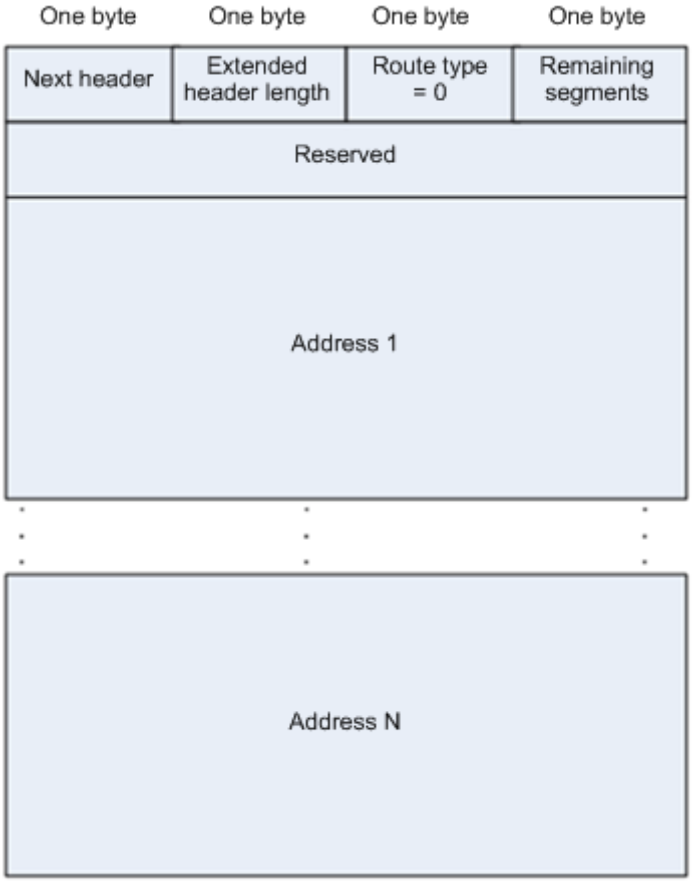


Рисунок 3-14.

В следующем примере описывается применение заголовка маршрутизации Type 0 (Рисунок 3-15).

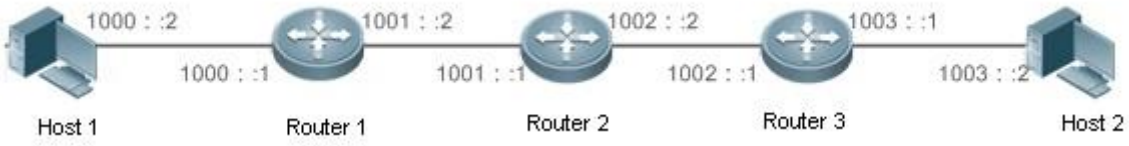


Рисунок 3-15.

Host 1 отправляет Host 2 пакет, указывающий промежуточные узлы маршрутизатор 2 и маршрутизатор 3. В следующей таблице перечислены изменения полей, связанные с заголовком IPv6 и заголовком маршрутизации в процессе пересылки.

Узел передачи	Поля в заголовке IPv6	Поля, связанные с заголовком маршрута Type 0
Host 1	Source address=1000::2 Destination address=1001::1 (Адрес Router 2)	Segments Left=2 Address 1=1002::1 (Адрес Router 3) Address 2=1003::2 (Адрес Host 2)
Router 1	No change	
Router 2	Source address=1000::2 Destination address=1002::1 (Адрес Router 3)	Segments Left=1 Address 1=1001::1 (Адрес Router 2) Address 2=1003::2 (Адрес Host 2)
Router 3	Source address=1000::2 Destination address=1003::2 (Адрес Host 2)	Segments Left=0 Address 1=1001::1 (Адрес Router 2) Address 1=1002::2 (Адрес Router 3)
Host 2	No change	

Процесс пересылки выполняется следующим образом:

1. Узел 1 отправляет пакет, в котором адресом назначения является адрес маршрутизатора 2 1001::1, заголовок маршрутизации типа 0 заполняется адресом маршрутизатора 3 1002::1 и адресом узла 2 1003::2, а значение поля Segments Left сегментов равно 2.
2. Маршрутизатор 1 пересылает этот пакет на маршрутизатор 2.
3. Маршрутизатор 2 изменяет адрес назначения в заголовке IPv6 на адрес 1 в заголовке маршрутизации. То есть, адрес назначения становится адресом 1002::1 маршрутизатора 3, адрес 1 в заголовке маршрутизации становится адресом маршрутизатора 2 1001::1, а значение левого поля сегментов становится 1. После внесения изменений маршрутизатор 2 пересылает пакет на маршрутизатор 3.
4. Маршрутизатор 3 изменяет адрес назначения в заголовке IPv6 на адрес 2 в заголовке маршрутизации. То есть, адрес назначения становится адресом узла 2 1003::2, адрес 2 в заголовке маршрутизации становится адресом маршрутизатора 3 1002::1, а значение левого поля сегментов становится 0. После внесения изменений маршрутизатор 3 пересылает пакет на узел 2.

Заголовок маршрутизации Type 0 может использоваться для инициирования DoS-атак. Как показано на Рисунке 3-16, узел 1 отправляет пакеты на узел 2 со скоростью 1 Мбит/с и удаляет заголовок маршрутизации, чтобы вызвать несколько петель обратной связи между маршрутизатором 2 и маршрутизатором 3 (50 раз с маршрутизатора 2 на маршрутизатор 3 и 49 раз с маршрутизатора 3 на маршрутизатор 2). В это время заголовок маршрутизации создает эффект усиления трафика: "50 Мбит/с с маршрутизатора 2 на маршрутизатор 3 и 49 Мбит/с с маршрутизатора 3 на маршрутизатор 2." Из-за этой проблемы безопасности RFC 5095 отменил заголовок маршрутизации Type 0.

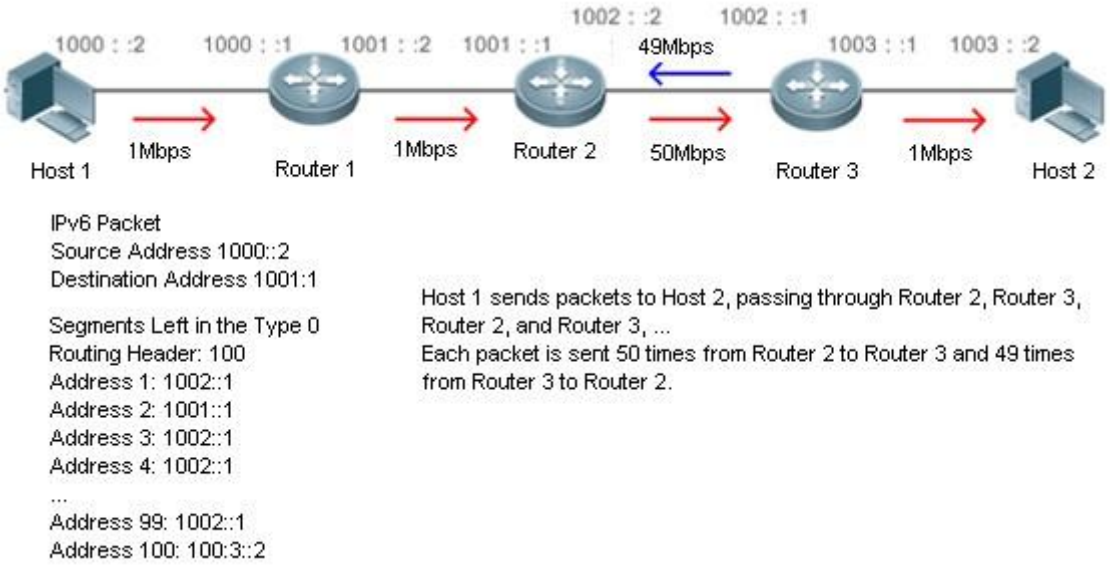


Рисунок 3-16.

3.3.7.2. Связанная конфигурация

Включение маршрутизации источника (Source routing) IPv6

- Заголовок маршрутизации Type 0 не поддерживается по умолчанию.
- Запустите команду **ipv6 source-route** в режиме глобальной конфигурации, чтобы включить маршрутизацию источника IPv6.

3.3.8. Ограничение скорости отправки сообщений об ошибках ICMPv6

3.3.8.1. Принцип работы

Узел назначения или промежуточный маршрутизатор отправляет сообщения ICMPv6, чтобы сообщить об ошибках, возникших во время пересылки и передачи пакетов данных IPv6. В основном существует четыре типа сообщений об ошибках: Destination Unreachable, Packet Too Big, Time exceeded и Parameter Problem.

При получении неверного пакета IPv6 устройство отбрасывает пакет и отправляет сообщение об ошибке ICMPv6 на исходный адрес IPv6. В случае dos атак на пакеты IPv6 устройство может непрерывно отвечать на сообщения об ошибках ICMPv6 до тех пор, пока ресурсы устройства не исчерпаны и, таким образом, не будут должным образом предоставляться услуги. Для решения этой проблемы можно ограничить скорость отправки сообщений об ошибках ICMPv6.

Если длина пересылаемого пакета IPv6 превышает MTU IPv6 исходящего интерфейса, маршрутизатор отбрасывает этот пакет IPv6 и отправляет обратно сообщение ICMPv6 Packet Too Big на исходный адрес IPv6. Это сообщение об ошибке в основном используется в процессе IPv6 PMTUD. Если скорость отправки сообщений об ошибках ICMPv6 ограничена из-за чрезмерного количества других сообщений об ошибках ICMPv6, сообщения ICMPv6 Packet Too Big могут быть отфильтрованы, что приведет к сбою IPv6 PMTUD. Поэтому рекомендуется ограничить скорость отправки пакетов ICMPv6 слишком большими сообщениями независимо от других сообщений об ошибках ICMPv6.

Несмотря на то, что пакеты перенаправления ICMPv6 не являются сообщениями об ошибках ICMPv6, рекомендуется ограничить их количество вместе с сообщениями об ошибках ICMPv6, за исключением сообщений Packet Too Big.

3.3.8.2. Связанная конфигурация

Настройка скорости отправки пакета ICMPv6 слишком больших сообщений

- Частота по умолчанию составляет 10 на 100 мс.
- Запустите команду **ipv6 icmp error-interval too-big**, чтобы настроить скорость отправки ICMPv6 Packet Too Big сообщений.

Настройка скорости отправки других сообщений об ошибках ICMPv6

- Частота по умолчанию составляет 10 на 100 мс.
- Выполните команду **ipv6 icmp error-interval** для настройки скорости отправки других сообщений об ошибках ICMPv6.

3.3.9. Ограничение перехода IPv6(IPv6 Hop Limit)

3.3.9.1. Принцип работы

Пакет данных IPv6 проходит через маршрутизаторы от исходного адреса и адреса назначения. Если настроен лимит перехода, он уменьшается на единицу при каждом прохождении пакета через маршрутизатор. Когда ограничение перехода уменьшается до 0, маршрутизатор отбрасывает пакет, чтобы предотвратить неограниченные возможности передачи бесполезного пакета по сети и потери пропускной способности сети. Ограничение перехода аналогично TTL IPv4.

3.3.9.2. Связанная конфигурация

Настройка предела операций IPv6

- Ограничение перехода IPv6 по умолчанию для устройства составляет 64.
- Выполните команду **ipv6 hop-limit**, чтобы настроить ограничение перехода IPv6 для устройства.

3.3.10. Преобразование из отправки пакетов NS в сети аутентификации VLAN

3.3.10.1. Принцип работы

В режиме аутентификации шлюза все подсети VLAN в Super VLAN по умолчанию являются сетями VLAN для аутентификации. Пользователи в сети аутентификации VLAN должны пройти аутентификацию для доступа к сети. После аутентификации на устройстве создается статическая запись ND. Поэтому при доступе к аутентифицированному пользователю устройству не нужно отправлять пакеты NS в VLAN аутентификации. Если устройство пытается получить доступ к пользователям в VLAN без аутентификации, ему нужно отправлять запросы NS только в VLAN без аутентификации.

В режиме аутентификации шлюза функция преобразования пакетов NS в сети аутентификации VLAN включена на устройстве по умолчанию. Если устройству требуется доступ к пользователям, не использующим аутентификацию, в сети аутентификации VLAN, отключите эту функцию.

3.3.10.2. Связанная конфигурация

Включение функции преобразования из отправки пакетов NS в сети аутентификации VLAN

- Запустите команду **ipv6 nd suppress-auth-vlan-ns** в режиме конфигурации интерфейса, чтобы включить функцию преобразования из отправки пакетов NS в сети аутентификации VLAN.
- Данный функционал включен по умолчанию.

- Эта функция поддерживается только на виртуальных интерфейсах коммутатора (SVI) и действует только в режиме аутентификации шлюза.

3.3.11. Шлюз по умолчанию в интерфейсе управления

3.3.11.1. Принцип работы

Шлюз по умолчанию настроен в интерфейсе управления для создания маршрута по умолчанию для этого интерфейса.

3.3.11.2. Связанная конфигурация

Настройка шлюза по умолчанию в интерфейсе управления

- Выполните команду **ipv6 gateway** *ipv6-address* в режиме конфигурации интерфейса, чтобы настроить шлюз по умолчанию в интерфейсе управления.
- По умолчанию в интерфейсе управления не настроен шлюз по умолчанию.

3.4. Настройка

Настройка	Описание и команда	
Настройка IPv6-адреса	(ОБЯЗАТЕЛЬНО) Используется для настройки адресов IPv6 и включения IPv6	
	ipv6 enable	Включает IPv6 в интерфейсе
	ipv6 address	Настраивает unicast-адрес IPv6 интерфейса
Настройка IPv6 NDP	(ОПЦИОНАЛЬНО) Используется для включения перенаправления IPv6 на интерфейсе	
	ipv6 redirects	Включает перенаправление IPv6 на интерфейсе
	(ОПЦИОНАЛЬНО) Используется для включения DAD	
	ipv6 nd dad attempts	Настраивает количество последовательных пакетов NS, отправленных DAD
	(ОПЦИОНАЛЬНО) Используется для настройки параметров ND	
	ipv6 nd reachable-time	Настройка доступного времени соседнего узла
	ipv6 nd prefix	Настройка префикса адреса, который будет объявляться в пакете RA

Настройка	Описание и команда	
Настройка IPv6 NDP	**ipv6 nd suppress-ra**	Включает подавление RA на интерфейсе
	(ОПЦИОНАЛЬНО) Используется для настройки максимального количества неразрешенных записей ND	
	ipv6 nd unresolved	Настраивает максимальное количество неразрешенных записей ND
	(ОПЦИОНАЛЬНО) Используется для настройки максимального количества соседей, полученных на интерфейсе	
	ipv6 nd cache interface-limit	Настраивает максимальное количество соседей, полученных на интерфейсе
Настройка MTU IPv6 на интерфейсе	(ОПЦИОНАЛЬНО) Используется для ограничения MTU пакетов IPv6, отправленных через интерфейс	
	ipv6 mtu	Настраивает MTU IPv6
Включение маршрута источника IPv6 (IPv6 Source Routing)	(ОПЦИОНАЛЬНО) Используется для включения маршрутизации источника IPv6	
	ipv6 source-route	Настройка устройства для пересылки пакетов IPv6 с заголовком маршрутизации
Настройка скорости отправки сообщений об ошибках ICMPv6	Опционально	
	ipv6 icmp error-interval too-big	Настройка скорости отправки пакетов ICMPv6 слишком больших сообщений
	ipv6 icmp error-interval	Настройка скорости отправки других сообщений об ошибках ICMPv6 и пакетов перенаправления ICMPv6
Настройка значения IPv6 Hop Limit	(ОПЦИОНАЛЬНО) Используется для ограничения числа переходов одноадресных пакетов IPv6, отправленных через интерфейс	
	ipv6 hop-limit	Настройка ограничения перехода IPv6

Настройка	Описание и команда	
Включение/выключение функции отказа отправки пакетов NS в сети VLAN аутентификации	(ОПЦИОНАЛЬНО) Используется для ограничения отправки пакетов NS в сети аутентификации VLAN в режиме аутентификации шлюза	
	ipv6 nd suppressauth-vlan-ns	Включает подавление широковещательной рассылки NS в сетях аутентификации VLAN
Настройка шлюза по умолчанию в интерфейсе управления	(ОПЦИОНАЛЬНО) Используется для настройки шлюза по умолчанию в интерфейсе управления	
	ipv6 gateway *ipv6-address*	Настройка шлюза по умолчанию в интерфейсе управления

3.4.1. Настройка IPv6-адреса

3.4.1.1. Результат конфигурации

Настройте IPv6-адрес интерфейса для реализации сетевой связи IPv6.

3.4.1.2. Этапы конфигурации

Включение IPv6 на интерфейсе

- (ОПЦИОНАЛЬНО) Если вы хотите включить поддержку протокола без настройки адреса IPv6, выполните команду **ipv6 enable**.

Настройка unicast-адреса IPv6-интерфейса

- Обязательно.

3.4.1.3. Проверка конфигурации

Запустите команду **show ipv6 interface**, чтобы проверить, действует ли настроенный адрес.

3.4.1.4. Связанные команды

Включение IPv6 на интерфейсе

Команда	**ipv6 enable**
Режим конфигурации	Режим конфигурации интерфейса

Встроенная подсказка	Протокол IPv6 можно включить на интерфейсе двумя способами: 1) выполнение команды **ipv6 enable** в режиме настройки интерфейса; 2) настройка адреса IPv6 на интерфейсе. **ПРИМЕЧАНИЕ:** если интерфейс связан с мультипротокольным объектом VRF, настроенным без семейства адресов IPv6, IPv6 не может быть включен на этом интерфейсе. IPv6 на этом интерфейсе можно включить только после настройки семейства адресов IPv6 для многопротокольной VRF. Если IPv6-адрес настроен на интерфейсе, IPv6 автоматически включается на этом интерфейсе. В этом случае протокол IPv6 нельзя отключить, даже если вы выполняете команду **no ipv6 enable**

Настройка unicast-адреса IPv6 интерфейса

Команда	**ipv6 address** *ipv6-address* / *prefix-length* **ipv6 address** ipv6-prefix / prefix-length **eui-64** **ipv6 address** prefix-name sub-bits / prefix-length [**eui-64**]
Описание параметров	*ipv6-address*: указывает адрес IPv6, который должен соответствовать формату адреса, определенному в RFC 4291. Разделенное двоеточием (:), каждое поле адреса состоит из 16 бит и представлено шестнадцатеричными символами. *ipv6-prefix*: указывает префикс адреса IPv6, который должен соответствовать формату адреса, определенному в RFC 4291. *prefix-length*: указывает длину префикса адреса IPv6, то есть часть, представляющую сеть в адресе IPv6. *prefix-name*: указывает имя универсального префикса. Указанный универсальный префикс используется для создания адреса интерфейса. *sub-bits*: указывает биты субпрефикса и биты хоста адреса, которые должны быть объединены с префиксами, предоставленными общим префиксом, указанным с параметром *prefix-name*. Это значение объединяется с универсальным префиксом для создания адреса интерфейса. Это значение должно быть в форме, указанной в RFC 4291. *eui-64*: указывает созданный IPv6-адрес, состоящий из настроенного префикса адреса и 64-битного идентификатора интерфейса
Режим конфигурации	Режим конфигурации интерфейса

Встроенная подсказка	**ПРИМЕЧАНИЕ:** если интерфейс связан с мультипротокольным объектом VRF, настроенным без семейства адресов IPv6, адрес IPv6 не может быть настроен для этого интерфейса. IPv6-адрес этого интерфейса можно настроить только после настройки семейства адресов IPv6 для многопротокольной VRF. Если интерфейс IPv6 создан и находится в состоянии готовности, система автоматически создает локальный адрес канала для этого интерфейса. IPv6-адрес интерфейса также может быть создан с помощью универсального механизма префиксов. То есть IPv6-адрес = Universal prefix + Sub prefix + Host bits. Универсальный префикс можно настроить, выполнив команду **ipv6 general-prefix** или выполнив функцию обнаружения префиксов клиента DHCPv6 (см. раздел 5. *Настройка DHCPv6*). Sub prefix + Host bits узла задаются параметрами *sub-bits* и *prefix-length* в команде **ipv6 address**. Если вы запускаете команду **no ipv6 address** без указания адреса, все адреса, настроенные вручную, будут удалены. Чтобы удалить настроенный адрес, выполните команду **no ipv6 address** *ipv6-prefix/prefix-length* **eui-64**

3.4.1.5. Пример конфигурации

Настройка адреса IPv6 в интерфейсе

Этапы конфигурации	Включите IPv6 на интерфейсе GigabitEthernet 0/0 и добавьте IPv6-адрес 2000::1 в интерфейс
	QTECH(config)#interface gigabitEthernet 0/0 QTECH(config-if-GigabitEthernet 0/0)#ipv6 enable QTECH(config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64
Проверка конфигурации	Выполните команду **show ipv6 interface**, чтобы убедиться, что адрес успешно добавлен в интерфейс GigabitEthernet 0/0
	QTECH(config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 INET6: 2000::1 [TENTATIVE], subnet is 2000::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds

	ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160-240> ND router advertisements live for 1800 seconds

3.4.2. Настройка IPv6 NDP

3.4.2.1. Результат конфигурации

Настройте атрибуты, связанные с NDP, например, включите перенаправление IPv6 и DAD.

3.4.2.2. Примечания

Подавление RA включено на интерфейсах по умолчанию. Чтобы настроить устройство для отправки пакетов RA, выполните команду **no ipv6 nd suppress-ra** в режиме конфигурации интерфейса.

3.4.2.3. Этапы конфигурации

Включение перенаправления IPv6 на интерфейсе

- (ОПЦИОНАЛЬНО) перенаправление IPv6 включено по умолчанию.
- Чтобы отключить перенаправление IPv6 на интерфейсе, выполните команду **no ipv6 redirects**.

Настройка количества последовательных пакетов NS, отправленных во время DAD

- Опционально.
- Чтобы запретить включение DAD для адресов IPv6 на интерфейсе или изменить количество последовательных пакетов NS, отправленных DAD, выполните команду **ipv6 nd dad attempts**.

Настройка доступного времени соседнего узла

- Опционально.
- Для изменения доступного времени соседа выполните команду **ipv6 nd reachable-time**.

Настройка префикса адреса для объявления в пакете RA

- По умолчанию префикс в пакете RA на интерфейсе — это префикс, настроенный в команде **ipv6 address** интерфейса.
- (Необязательно) Выполните команду **ipv6 nd prefix**, чтобы добавить или удалить префиксы и параметры префиксов, которые могут быть объявлены.

Включение/выключение подавления RA на интерфейсе

- Опционально.
- Чтобы настроить устройство для отправки пакетов RA, выполните команду **no ipv6 nd suppress-ra**.

Настройка максимального количества неразрешенных записей ND

- Опционально.
- Если из-за сканирующих атак создается большое количество неразрешенных записей ND, выполните команду **ipv6 nd unresolved**, чтобы ограничить число неразрешенных соседей.

Настройка максимального количества записей ND, полученных в интерфейсе

- Опционально.
- Если количество хостов IPv6 контролируется, выполните команду **ipv6 nd cache interface-limit**, чтобы ограничить количество соседей, обученных на интерфейсе. Это предотвращает попадание атак, полученных с помощью функции изучения ND, в пространство памяти и влияет на производительность устройства.

3.4.2.4. Проверка конфигурации

Выполните следующие команды для проверки правильности конфигурации:

- **show ipv6 interface** *interface-type interface-num*: проверьте, действуют ли такие конфигурации, как функция перенаправления, время доступности соседнего узла и интервал отправки NS.
- **show ipv6 interface** *interface-type interface-num* ra-inifo: проверьте правильность префикса и другой информации, настроенной для пакетов RA.
- **show run**

3.4.2.5. Связанные команды

Включение перенаправления IPv6 на интерфейсе

Команда	**ipv6 redirects**
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Все сообщения об ошибках ICMPv6 передаются с ограниченной скоростью передачи. По умолчанию 10 — максимальное количество сообщений об ошибках ICMPv6 передаваемых в секунду (10 пакетов в секунду)

Настройка количества последовательных пакетов NS, отправленных во время DAD

Команда	**ipv6 nd dad attempts** *value*
Описание параметров	*value*: указывает количество пакетов NS
Режим конфигурации	Режим конфигурации интерфейса

Встроенная подсказка	Перед настройкой адреса IPv6 на интерфейсе необходимо включить DAD. Затем адрес находится в предварительном состоянии. Если DAD не обнаруживает конфликта адресов, этот адрес можно использовать. Если обнаружен конфликт адресов и идентификатор интерфейса этого адреса использует EUI-64, на этом канале существуют дублирующие адреса уровня связи. В этом случае система автоматически отключает этот интерфейс для предотвращения операций, связанных с IPv6 на этом интерфейсе). В это время необходимо настроить новый адрес и перезапустить интерфейс, чтобы снова включить DAD. Когда интерфейс переходит из состояния вниз в состояние вверх, DAD снова включается для адресов в этом интерфейсе

Настройка времени доступности соседнего узла

Команда	**ipv6 nd reachable-time** *milliseconds*
Описание параметров	*milliseconds*: указывает время доступности соседа в диапазоне от 0 до 3 600 000. Единица измерения — миллисекунда. Значение по умолчанию — 30 с
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Устройство обнаруживает недоступных соседей в соответствии с настроенным временем доступа. Чем короче настроенное время доступа, тем быстрее устройство обнаруживает недоступных соседей, но тем больше оно потребляет полосу пропускания сети и ресурсы устройства. Поэтому не рекомендуется устанавливать это значение слишком маленьким. Настроенное значение объявляется в пакете RA и также используется на устройстве. Если значение равно 0, на устройстве не указано время доступа, и рекомендуется использовать значение по умолчанию

Настройка префикса адреса для объявления в пакете RA

Команда	**ipv6 nd prefix {***ipv6-prefix/prefix-length* | **default**} [[*valid-lifetime* { **infinite** | *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite** {**infinite** | *preferred-lifetime*}]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]
Описание параметров	*ipv6-prefix*: указывает идентификатор сети IPv6, который должен соответствовать формату представления адреса в RFC 4291. *prefix-length*: указывает длину префикса адреса IPv6. Перед префиксом необходимо добавить косую черту (/). *valid-lifetime*: указывает период, в течение которого хост, получающий префикс пакета RA, считает префикс допустимым. Диапазон значений от 0 до 4 294 967 295. Значение по умолчанию: 30 дней. *preferred-lifetime*: указывает период, в течение которого хост, получающий префикс пакета RA, считает префикс допустимым. Диапазон значений от 0 до 4 294 967 295. Значение по умолчанию: 7 дней. **at** *valid-date preferred-date*: указывает допустимую дату и предпочитаемый срок, настроенный для префикса RA. Используется формат *dd+mm+yyyy+hh+mm*. **infinite**: указывает на то, что префикс действителен навсегда. **default**: указывает, что используется конфигурация параметров по умолчанию. **no-advertise**: указывает, что префикс не объявляется маршрутизатором. **off-link**: если префикс адреса назначения в пакете IPv6, отправленном хостом, совпадает с настроенным префиксом, устройство будет рассматривать адрес назначения по той же ссылке и непосредственно доступен. Этот параметр указывает, что этот префикс не требует определения по каналу. **no-autoconfig**: указывает, что префикс в пакете RA, полученном хостом, не может использоваться для автоматической настройки адреса
Режим конфигурации	Режим конфигурации интерфейса

Встроенная подсказка	Эту команду можно использовать для настройки параметров, связанных с каждым префиксом, включая возможность объявления этого префикса. По умолчанию пакет RA использует префикс, настроенный с помощью команды ipv6-адреса. Запустите команду **ipv6 nd prefix**, чтобы добавить другие префиксы. Выполните команду **ipv6 nd prefix default**, чтобы настроить параметры интерфейса по умолчанию. То есть, если при добавлении префикса не указан ни один параметр, используйте параметры, настроенные в команде **ipv6 nd prefix default** по умолчанию в качестве параметров нового префикса. Конфигурации параметров по умолчанию отменятся после того, как для префикса будет указан параметр. То есть, при использовании команды **ipv6 nd prefix default** по умолчанию для изменения настроек параметров по умолчанию, только префикс, настроенный для изменений параметров по умолчанию и конфигураций префикса, остается прежним. **at** *valid-date preferred-date*: можно указать допустимую дату префикса двумя способами: 1) указание фиксированного времени для каждого префикса в пакете RA; 2) указание срока. Во втором методе действительная дата префикса в каждом пакете RA уменьшается до 0

Включение/выключение подавления RA на интерфейсе

Команда	**ipv6 nd suppress-ra**
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы включить подавление RA на интерфейсе, выполните команду **ipv6 suppress-ra**

Настройка максимального количества неразрешенных записей ND

Команда	**ipv6 nd unresolved** *number*
Описание параметров	*number*: указывает максимальное количество неразрешенных записей ND
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Чтобы предотвратить создание большим количеством неразрешенных записей ND и занимающих ресурсы ввода злоумышленниками, можно ограничить количество неразрешенных записей ND

Настройка максимального количества записей ND, полученных в интерфейсе

Команда	**ipv6 nd cache interface-limit** *value*
Описание параметров	*value*: указывает максимальное количество соседних устройств, полученных интерфейсом
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Ограничение количества записей ND, полученных в интерфейсе, может предотвратить атаки злоумышленников-соседей. Если это число не ограничено, на устройстве будет создано большое количество записей ND, занимающих слишком много места в памяти. Настроенное значение должно быть равно или больше числа записей ND, полученных интерфейсом. В противном случае конфигурация не вступит в силу. Конфигурация зависит от емкости ввода ND, поддерживаемой устройством

3.4.2.6. Пример конфигурации

Включение перенаправления IPv6 на интерфейсе

Этапы конфигурации	Включите перенаправление IPv6 на интерфейсе GigabitEthernet 0/0
	QTECH(config-if-GigabitEthernet 0/0)#ipv6 redirects
Проверка конфигурации	Выполните команду **show ipv6 interface**, чтобы проверить результат
	QTECH#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds

	ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160-240> ND router advertisements live for 1800 seconds

Настройка IPv6 DAD

Этапы конфигурации	Настройте интерфейс для отправки DAD трех последовательных пакетов NS
	QTECH(config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3
Проверка конфигурации	Выполните команду **show ipv6 interface**, чтобы проверить результат
	QTECH#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:0:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 3 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160-240> ND router advertisements live for 1800 seconds QTECH(config-if-GigabitEthernet 0/0)#

Настройка информации префикса в пакете RA

Этапы конфигурации	Добавьте префикс 1234:/64 к интерфейсу GigabitEthernet 0/0
	QTECH(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/64

Проверка конфигурации	Выполните команду **show ipv6 interface**, чтобы проверить результат
	QTECH#show ipv6 interface gigabitEthernet 0/0 ra-info GigabitEthernet 0/0: DOWN (RA is suppressed) RA timer is stopped waits: 0, initcount: 0 statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0 Link-layer address: 00:00:00:00:00:00 Physical MTU: 1500 ND router advertisements live for 1800 seconds ND router advertisements are sent every 200 seconds<160-240> Flags: !M!O, Adv MTU: 1500 ND advertised reachable time is 0 milliseconds ND advertised retransmit time is 0 milliseconds ND advertised CurHopLimit is 64 Prefixes: <total: 1> 1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)

Настройка пакетов RA для получения префиксов из пула префиксов

Этапы конфигурации	Настройте пакеты RA на получение префиксов из пула префиксов "ra-pool"
	QTECH(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool
Проверка конфигурации	Выполните команду **show run**, чтобы проверить результат
	QTECH(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0 Building configuration... Current configuration : 125 bytes interface GigabitEthernet 0/0 ipv6 enable no ipv6 nd suppress-ra peel default ipv6 pool ra-pool !

Отключение подавления RA

Этапы конфигурации	Отключите подавление PA на интерфейсе
	QTECH(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra
Проверка конфигурации	Выполните команду **show run**, чтобы проверить результат
	QTECH(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0 Building configuration... Current configuration : 125 bytes interface GigabitEthernet 0/0 ipv6 enable no ipv6 nd suppress-ra !

Настройка максимального количества неразрешенных записей ND

Этапы конфигурации	Установите максимальное количество неразрешенных записей ND равным 200
	QTECH(config)# ipv6 nd unresolved 200
Проверка конфигурации	Выполните команду **show run**, чтобы проверить результат
	QTECH#show run ipv6 nd unresolved 200 !

Настройка максимального количества записей ND, полученных в интерфейсе

Этапы конфигурации	Установите максимальное количество записей ND, полученных на интерфейсе, равным 100
	QTECH(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100

Проверка конфигурации	Выполните команду **show run**, чтобы проверить результат
	QTECH#show run ! interface GigabitEthernet 0/1 ipv6 nd cache interface-limit 100 !

3.4.3. Настройка MTU IPv6 на интерфейсе

3.4.3.1. Результат конфигурации

В соответствии со схемой сети, настройте корректный адрес IPv6, чтобы избежать потери пакетов.

3.4.3.2. Примечания

MTU IPv6 интерфейса должен быть меньше или равен MTU-интерфейса. Диапазон IPv6 MTU составляет от 1280 до 1500.

3.4.3.3. Этапы конфигурации

Настройка MTU IPv6 интерфейса

- Опционально.
- Если минимальный размер MTU в Интернете меньше MTU IPv6-интерфейса, используйте эту конфигурацию для установки правильного MTU-интерфейса.

3.4.3.4. Проверка конфигурации

- Запустите команду **show run** или **show ipv6 interface**, чтобы проверить правильность конфигурации.
- Захват локально отправленных пакетов IPv6, длина которых превышает MTU IPv6. Результат захвата пакетов показывает, что пакет IPv6 фрагментирован на основе MTU IPv6-интерфейса.

3.4.3.5. Связанные команды

Настройка MTU IPv6-интерфейса

Команда	**ipv6 mtu** *bytes*
Описание параметров	*bytes*: указывает MTU пакета IPv6 в диапазоне от 1280 до 1500. Единица измерения — байт
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

3.4.3.6. Пример конфигурации

Настройка MTU IPv6-интерфейса

Этапы конфигурации	Измените IPv6 MTU-интерфейса GigabitEthernet 0/0 на 1300
	QTECH(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
Проверка конфигурации	Выполните команду **show ipv6 interface**, чтобы проверить результат
	QTECH(config-if-GigabitEthernet 0/0)#show ipv6 interface interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 08:c6:b3:f1:17:61 INET6: FE80::2D0:F8FF:FE22:3347 [TENTATIVE], subnet is FE80::/64 INET6: 1020::1 [TENTATIVE], subnet is 1020::/64 INET6: 1023::1 [TENTATIVE], subnet is 1023::/64 Joined group address(es): MTU is 1300 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160-240> ND router advertisements live for 1800 seconds

3.4.4. Включение маршрута источника IPv6 (IPv6 Source Routing)

3.4.4.1. Результат конфигурации

RFC 5095 отменил заголовок маршрутизации типа 0. Устройства QTECH по умолчанию не поддерживают заголовок маршрутизации типа 0. Администратор может выполнить команду **ipv6 source-route** в режиме глобальной конфигурации, чтобы включить маршрут источника IPv6.

3.4.4.2. Этапы конфигурации

Включение маршрута источника (Source routing) IPv6

- Опционально.
- Чтобы включить маршрут источника IPv6, выполните команду **ipv6 source-route**.

3.4.4.3. Проверка конфигурации

Устройство может должным образом пересылать пакеты с заголовком маршрутизации Type 0.

3.4.4.4. Связанные команды

Включение маршрутизации источника IPv6

Команда	**ipv6 source-route**
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Поскольку заголовок типа 0 может привести к атакам DoS на устройство, устройство не пересылает пакеты IPv6 с заголовком маршрутизации по умолчанию, а обрабатывает пакеты IPv6, сам по себе являясь конечным адресом назначения и заголовком маршрутизации типа 0

3.4.4.5. Пример конфигурации

Включение маршрутизации источника IPv6

Этапы конфигурации	Включить маршрутизацию источника IPv6
	QTECH(config)#ipv6 source-route
Проверка конфигурации	Выполните команду **show run**, чтобы проверить результат
	QTECH#show run | inc ipv6 source-route ipv6 source-route

3.4.5. Настройка скорости отправки сообщений об ошибках ICMPv6

3.4.5.1. Результат конфигурации

Настройка скорости отправки сообщений об ошибках ICMPv6.

3.4.5.2. Этапы конфигурации

Настройка скорости отправки пакета ICMPv6 слишком больших сообщений

- Опционально.
- Если устройство получает множество пакетов IPv6 с длиной пакета, превышающей IPv6 MTU исходящего интерфейса, и, таким образом, отправляет большое количество ICMPv6 Packet Too Big сообщений, которые потребляют много ресурсов ЦП, запустите команду **ipv6 icmp error-interval too-big** с слишком большим интервалом ошибок, чтобы ограничить скорость отправки этого сообщения об ошибке.

Настройка скорости отправки других сообщений об ошибках ICMPv6

- Опционально.
- Если устройство получает множество невалидных пакетов IPv6 и, таким образом, генерирует много сообщений об ошибках ICMPv6, выполните команду **ipv6 icmp error-interval**, чтобы ограничить скорость отправки сообщений об ошибках ICMPv6. Эта команда не влияет на скорость отправки ICMPv6 Packet Too Big сообщений.

3.4.5.3. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить результат.

3.4.5.4. Связанные команды

Настройка скорости отправки пакета ICMPv6 слишком больших сообщений

Команда	**ipv6 icmp error-interval too-big** *milliseconds* [*bucket-size*]
Описание параметров	*milliseconds*: указывает период обновления контейнера маркеров в диапазоне от 0 до 2 147 483 647. Единица измерения — миллисекунда. Значение по умолчанию: 100. Если значение равно 0, скорость отправки сообщений об ошибках ICMPv6 не ограничена. *bucket-size*: указывает количество маркеров в контейнере для маркеров в диапазоне от 1 до 200. Значение по умолчанию — 10
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Для предотвращения DoS-атак используйте алгоритм контейнера маркеров, чтобы ограничить скорость отправки сообщений об ошибках ICMPv6. Если длина пересылаемого пакета IPv6 превышает MTU IPv6 исходящего интерфейса, маршрутизатор отбрасывает этот пакет IPv6 и отправляет обратно сообщение ICMPv6 Packet Too Big на исходный адрес IPv6. Это сообщение об ошибке в основном используется в процессе IPv6 PMTUD. Если другие сообщения об ошибках ICMPv6 являются чрезмерными, невозможно отправить пакет ICMPv6 Packet Too Big, что приводит к сбою IPv6 PMTUD. Поэтому рекомендуется ограничить скорость отправки пакетов ICMPv6 Packet Too Big независимо от других сообщений об ошибках ICMPv6. Поскольку точность таймера составляет 10 мс, рекомендуется установить интервал обновления контейнера маркеров на целое число, кратное 10 мс. Если период обновления контейнера маркеров находится в диапазоне от 0 до 10, фактический период обновления составляет 10 мс. Например, если скорость отправки установлена на 1 каждые 5 мс, два сообщения об ошибках отправляются каждые 10 мс в реальных ситуациях. Если период обновления контейнера маркеров не является целым числом, кратным 10 мс, он автоматически преобразуется в целое число, кратное 10 мс.

Встроенная подсказка	Например, если для скорости отправки установлено значение 3 каждые 15 мс, два ключа обновляются каждые 10 мс в реальных ситуациях

Настройка скорости отправки других сообщений об ошибках ICMPv6

Команда	**ipv6 icmp error-interval** *milliseconds* [*bucket-size*]
Описание параметров	*milliseconds*: указывает период обновления контейнера маркеров в диапазоне от 0 до 2 147 483 647. Единица измерения — миллисекунда. Значение по умолчанию — 100. Если значение равно 0, скорость отправки сообщений об ошибках ICMPv6 не ограничена. *bucket-size*: указывает количество маркеров в контейнере для маркеров в диапазоне от 1 до 200. Значение по умолчанию — 10
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Для предотвращения DoS-атак используйте алгоритм контейнера маркеров, чтобы ограничить скорость отправки сообщений об ошибках ICMPv6. Поскольку точность таймера составляет 10 мс, рекомендуется установить интервал обновления контейнера маркеров на целое число, кратное 10 мс. Если период обновления контейнера маркеров находится в диапазоне от 0 до 10, фактический период обновления составляет 10 мс. Например, если скорость отправки установлена на 1 каждые 5 мс, два сообщения об ошибках отправляются каждые 10 мс в реальных ситуациях. Если период обновления контейнера маркеров не является целым числом, кратным 10 мс, он автоматически преобразуется в целое число, кратное 10 мс. Например, если для скорости отправки установлено значение 3 каждые 15 мс, два ключа обновляются каждые 10 мс в реальных ситуациях

3.4.5.5. Пример конфигурации

Настройка скорости отправки сообщений об ошибках ICMPv6

Этапы конфигурации	Установите скорость отправки слишком большого сообщения ICMPv6 на уровне 100 пакетов в секунду, а для других сообщений об ошибках ICMPv6 — на уровне 10 пакетов в секунду
	QTECH(config)#ipv6 icmp error-interval too-big 1000 100 QTECH(config)#ipv6 icmp error-interval 1000 10
Проверка конфигурации	Выполните команду **show running-config**, чтобы проверить результат

	QTECH#show running-config | include ipv6 icmp error-interval ipv6 icmp error-interval 1000 10 ipv6 icmp error-interval too-big 1000 100

3.4.6. Настройка значения IPv6 Hop Limit

3.4.6.1. Результат конфигурации

Настройте количество переходов одноадресного пакета для предотвращения неограниченной передачи пакета.

3.4.6.2. Этапы конфигурации

Настройка предела операций IPv6

- Опционально.
- Чтобы изменить количество переходов одноадресного пакета, выполните команду **ipv6 hop-limit** *value*.

3.4.6.3. Проверка конфигурации

- Выполните команду **show running-config**, чтобы проверить правильность конфигурации.
- Захват одноадресных пакетов IPv6, отправленных хостом. Результат захвата пакетов показывает, что значение поля ограничения перехода в заголовке IPv6 совпадает с настроенным ограничением перехода.

3.4.6.4. Связанные команды

Настройка предела операций IPv6

Команда	**ipv6 hop-limit** *value*
Описание параметров	*value*: указывает количество переходов одноадресного пакета, отправленного устройством. Диапазон значений от 1 до 255
Режим конфигурации	Режим глобальной конфигурации

3.4.6.5. Пример конфигурации

Настройка предела хопов IPv6

Этапы конфигурации	Измените ограничение перехода IPv6 устройства на 250
	QTECH(config)#ipv6 hop-limit 250
Проверка конфигурации	Выполните команду **show running-config**, чтобы проверить результат

	QTECH#show running-config ipv6 hop-limit 254

3.4.7. Включение/выключение функции отказа отправки пакетов NS в сети VLAN аутентификации

3.4.7.1. Результат конфигурации

Включение или отключение функции отказа отправки пакетов NS в сети VLAN аутентификации в SVI.

3.4.7.2. Примечания

Конфигурация поддерживается только в SVI и действует только в режиме аутентификации шлюза.

3.4.7.3. Этапы конфигурации

Включение/выключение функции отказа отправки пакетов NS в сети VLAN аутентификации

- Опционально.
- В режиме аутентификации шлюза выполните команду **no ipv6 nd suppressauth-vlan-ns**, чтобы устройство могло отправлять пакеты NS в сети VLAN аутентификации.

3.4.7.4. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить правильность конфигурации.

3.4.7.5. Связанные команды

Включение/выключение функции отказа отправки пакетов NS в сети VLAN аутентификации

Команда	**ipv6 nd suppress-auth-vlan-ns**
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Для отключения этой функции используйте форму **no** данной команды

3.4.7.6. Пример конфигурации

Отключение функции отказа отправки пакетов NS в сети VLAN аутентификации

Этапы конфигурации	Отключите функцию отказа отправки пакетов NS в сети VLAN аутентификации
	QTECH(config-if-VLAN 2)#no ipv6 nd suppress-auth-vlan-ns

Проверка конфигурации	Запустите команду **show running-config interface vlan 2**, чтобы проверить результат
	QTECH#show running-config interface vlan 2 no ipv6 nd suppress-auth-vlan-ns

3.4.8. Настройка шлюза по умолчанию в интерфейсе управления

3.4.8.1. Результат конфигурации

Настройте шлюз по умолчанию в интерфейсе управления. Создается маршрут по умолчанию, при этом исходящий интерфейс является интерфейсом управления, а следующий переход — настроенным шлюзом.

3.4.8.2. Примечания

Конфигурация поддерживается только в интерфейсе управления.

3.4.8.3. Этапы конфигурации

Настройка шлюза по умолчанию в интерфейсе управления

- Опционально.
- Чтобы настроить маршрут по умолчанию для интерфейса управления, выполните команду **ipv6 gateway**.

3.4.8.4. Проверка конфигурации

Выполните команду **show running-config**, чтобы проверить правильность конфигурации.

3.4.8.5. Связанные команды

Настройка шлюза по умолчанию в интерфейсе управления

Команда	**ipv6 gateway** *ipv6-address*
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Эта команда поддерживается только в интерфейсе управления

3.4.8.6. Пример конфигурации

Настройка шлюза по умолчанию в интерфейсе управления.

Этапы конфигурации	Установить шлюз по умолчанию интерфейса управления на 2000::1
	QTECH(config)# interface mgmt 0 QTECH(config-mgmt)# ipv6 gateway 2000::1

Проверка конфигурации	Запустите команду **show running-config interface vlan 2**, чтобы проверить результат
	QTECH#show running-config interface mgmt 0 Ipv6 gateway 2000::1

3.5. Контроль состояния

3.5.1. Очистка

ВНИМАНИЕ: ВЫПОЛНЕНИЕ КОМАНД CLEAR МОЖЕТ ПРИВЕСТИ К ПОТЕРЕ ВАЖНОЙ ИНФОРМАЦИИ И, СЛЕДОВАТЕЛЬНО, ПРЕРЫВАНИЮ РАБОТЫ СЛУЖБ.

Описание	Команда
Очищает динамически изученные соседние области	**clrear ipv6 neighbors** [**vrf** *vrf-name*] [**oob**] [*interface-id*]

3.5.2. Отображение

Описание	Команда
Отображение информации IPv6-интерфейса	**show ipv6 interface** [[*interface-id*] [ra-info]] [brief [*interface-id*]]
Отображение информации о соседе	**show ipv6 neighbors [vrf** *vrf-name*] [**verbose**] [*interfaceid*] [*ipv6-address*] [static] [oob]
Отображает информацию в таблице маршрутизации IPv6	**show ipv6 route [vrf** vrf-name] [**static | local | connected | bgp | rip | ospf | isis]**

3.5.3. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому, отключите отладочный коммутатор сразу после использования.

Описание	Команда
Включение дебаг сообщений записи ND	**debug ipv6 nd**

4. НАСТРОЙКА DHCP

4.1. Обзор

Протокол динамической конфигурации хоста (DHCP) — это протокол LAN, на базе пользовательских датаграмм (UDP) для динамического назначения сетевых IP-адресов и сопутствующих параметров.

DHCP работает в режиме клиент-сервер. DHCP-клиент отправляет на сервер DHCP-запрос на получение IP-адреса и других конфигураций. Если клиент DHCP и сервер DHCP находятся не в одной подсети, то для пересылки запроса DHCP и ответа на пакеты требуется DHCP Relay.

4.1.1. Протоколы и стандарты

- RFC2131: протокол динамической конфигурации хоста.
- RFC2132: параметры DHCP и расширения поставщика BOOTP.
- RFC3046: опция информации о ретрансляторе DHCP.

4.2. Применение

Применение	Описание
Предоставление службы DHCP в локальной сети	Назначает IP-адреса клиентам в локальной сети
Включение клиента DHCP	Включите клиент DHCP
Применение правила AM на сервере DHCP	Применение DHCP-сервера в среде Super VLAN
Настройка DHCP Relay в проводной сети	В проводной сети пользователи из разных сегментов сети запрашивают IP-адреса
Применение правила AM на DHCP	В сети Super VLAN пользователи из разных сегментов сети запрашивают IP-адреса

4.2.1. Предоставление службы DHCP в локальной сети

4.2.1.1. Сценарий

Назначьте IP-адреса четырем пользователям локальной сети.

Например, назначьте IP-адреса пользователям 1, 2, 3 и 4, как показано на следующем Рисунке.

- Четыре пользователя подключены к серверу S через устройства A, B, C и D.

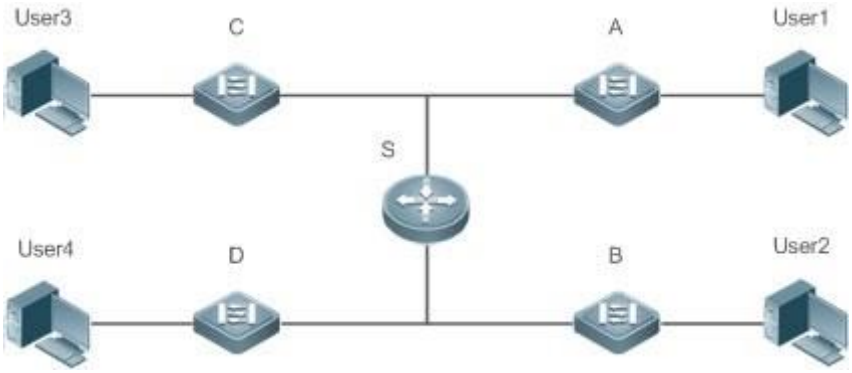


Рисунок 4-1.

S — это исходящий шлюз, работающий как DHCP-сервер.

A, B, C и D являются коммутаторами доступа, которые позволяют осуществлять прозрачную передачу на уровне 2.

Пользователь 1, пользователь 2, пользователь 3 и пользователь 4 являются пользователями локальной сети.

4.2.1.2. Описание

- Включите сервер DHCP на сервере S.
- Настройте прозрачную передачу VLAN уровня 2 на A, B, C и D.
- Пользователь 1, пользователь 2, пользователь 3 и пользователь 4 инициируют запросы клиента DHCP.

4.2.2. Включение клиента DHCP

4.2.2.1. Сценарий

Для назначения IP-адресов получите доступ к коммутаторам A, B, C и D на сервере S запроса локальной сети.

Например, включите DHCP Client на интерфейсах A, B, C и D для запроса IP-адресов, как показано на следующем Рисунке.

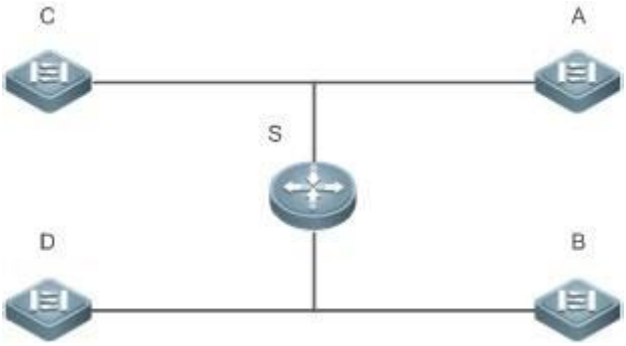


Рисунок 4-2.

S — это исходящий шлюз, работающий как DHCP-сервер.

A, B, C и D являются коммутаторами доступа с включенным клиентом DHCP на интерфейсах.

4.2.2.2. Описание

- Включите сервер DHCP на сервере S.

- Включите DHCP-клиент на интерфейсах A, B, C и D.

4.2.3. Применение правила AM на сервере DHCP

4.2.3.1. Сценарий

Как показано на Рисунке 4-3, создайте Super VLAN, настройте правило AM и включите сервер DHCP на основном коммутаторе A. B — коммутатор агрегации, C — коммутатор доступа и D — устройство беспроводного доступа. Требования перечислены ниже:

- Динамическое назначение IP-адресов на основе VLAN и порта.
- Назначать IP-адреса статически на основе VLAN.
- Динамическое назначение IP-адресов на основе правила AM по умолчанию.

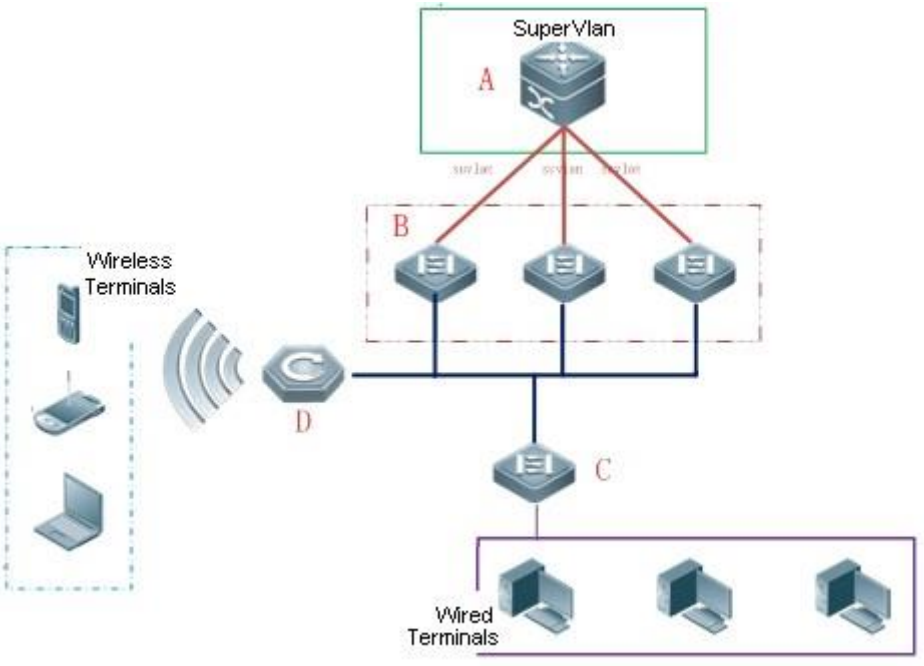


Рисунок 4-3. Применение правила AM на сервере DHCP

A — это основное устройство.

B — устройство агрегации.

C — это устройство проводного доступа.

D — это устройство беспроводного доступа.

4.2.3.2. Описание

- Настройте правило AM, включите сервер DHCP и создайте Super VLAN на A.
- Создайте VLAN на B и C для прозрачной передачи пакетов DHCP от проводных пользователей на A для запроса IP-адресов.
- Включите функцию беспроводной связи на D для прозрачной передачи пакетов DHCP от беспроводных пользователей на A для запроса IP-адресов.

4.2.4. Настройка DHCP Relay в проводной сети

4.2.4.1. Сценарий

Как показано на следующем Рисунке, коммутаторы C и D являются устройствами доступа для пользователей в сетях VLAN 10 и VLAN 20 соответственно. Коммутатор B является шлюзом, а коммутатор A — основным устройством. Требования перечислены ниже:

Коммутатор A работает в качестве DHCP-сервера для динамического назначения IP-адресов различных сегментов сети пользователям в различных сетях VLAN.

Пользователи в сетях VLAN 10 и VLAN 20 динамически получают IP-адреса.

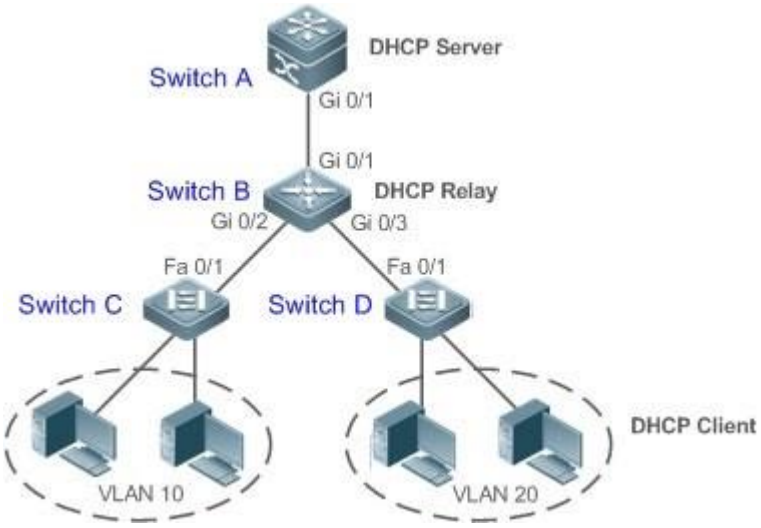


Рисунок 4-4. DHCP Relay

Коммутаторы C и D являются устройствами доступа.

Коммутатор B является шлюзом.

Коммутатор A является основным устройством.

4.2.4.2. Описание

- Настройте связь уровня 2 между коммутатором B и коммутатором C, а также между коммутатором B и коммутатором D.
- На коммутаторе B укажите адрес сервера DHCP и включите функцию DHCP Relay.
- На коммутаторе A создайте пулы адресов DHCP для VLAN 10 и VLAN 20 соответственно и включите сервер DHCP.

4.2.5. Применение правила AM на DHCP Relay

4.2.5.1. Сценарий

Как показано на Рисунке 4-5, A — это сервер DHCP, B — основной коммутатор, настроенный на Super VLAN, правило AM и ретрансляцию DHCP, C — коммутатор агрегации, D — коммутатор доступа и E — устройство беспроводного доступа. Требования перечислены ниже:

- На основании правила AM-порта VLAN-агент ретрансляции DHCP выбирает адрес подсети в качестве Giaddress пакетов ретрансляции и пересылает их на сервер DHCP для запроса IP-адреса клиента.

- В соответствии с правилом AM по умолчанию агент ретрансляции DHCP выбирает адрес подсети в качестве адреса для ретрансляции пакетов и пересылает их на сервер DHCP для запроса IP-адреса клиента.

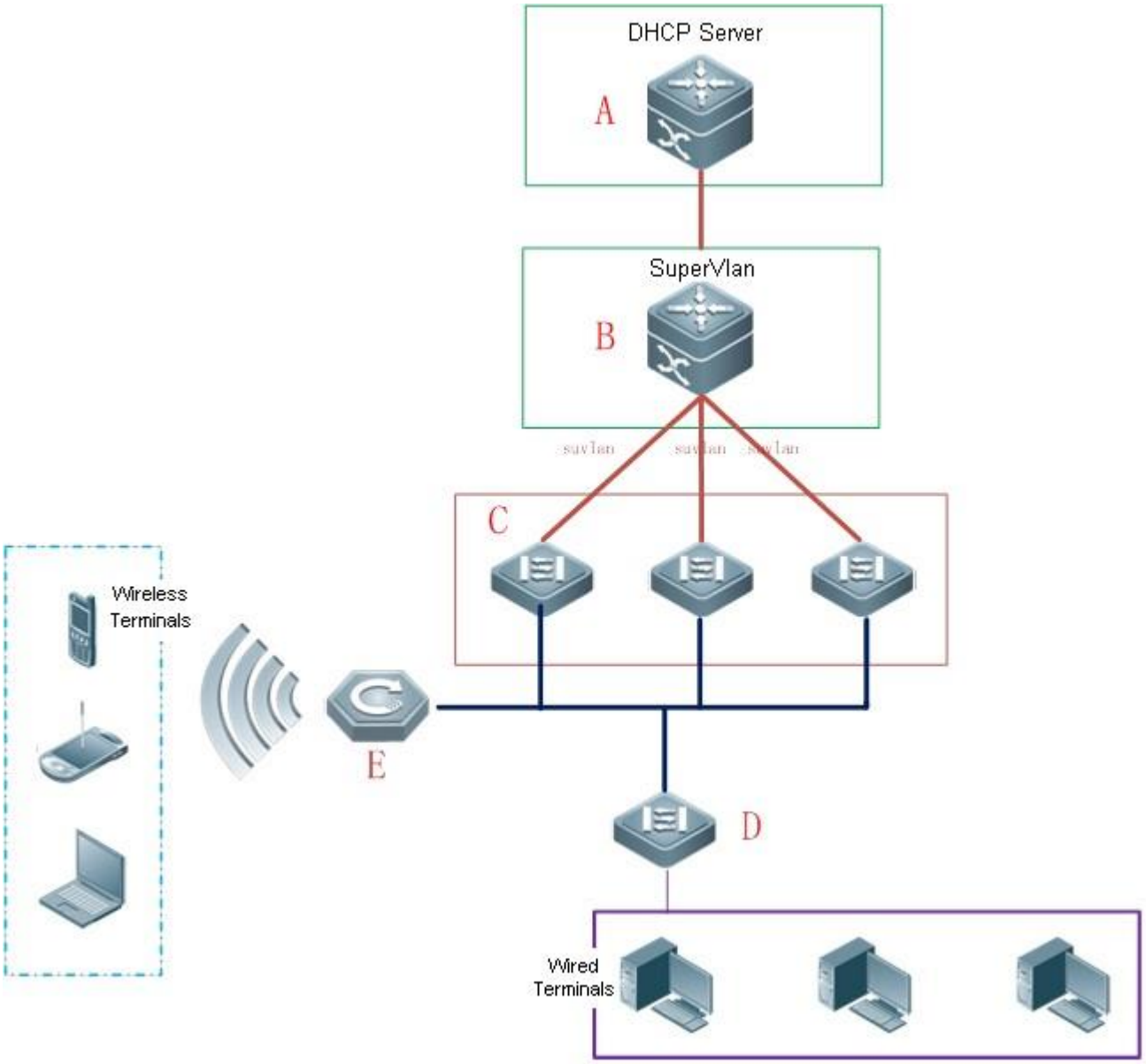


Рисунок 4-5. Применение правила AM на DHCP Relay

A — это основное устройство.

B — это основное устройство.

C — это устройство агрегации.

D — это устройство проводного доступа.

E — это устройство беспроводного доступа.

4.2.5.2. Описание

- Включите сервер DHCP на A.
- Настройте правило AM, включите DHCP Relay и создайте Super VLAN на B.

- Создайте VLAN на C и D для прозрачной передачи пакетов DHCP от проводных пользователей в B для запроса IP-адресов.
- Включите функцию беспроводной связи на E для прозрачной передачи пакетов DHCP от беспроводных пользователей в B для запроса IP-адресов.

4.3. Ключевые особенности

4.3.1. Базовые концепции

Сервер DHCP

На основе RFC 2131 DHCP-сервер QTECH назначает IP-адреса клиентам и управляет этими IP-адресами.

Клиент DHCP

Клиент DHCP позволяет устройству автоматически получать IP-адрес и конфигурации с сервера DHCP.

DHCP Relay

Если клиент DHCP и сервер DHCP находятся не в одной подсети, то для пересылки запроса DHCP и ответа на пакеты требуется DHCP Relay.

Аренда

Аренда — это период времени, указанный DHCP-сервером для клиента для использования назначенного IP-адреса. IP-адрес активен при аренде с клиентом. Перед истечением срока аренды клиенту необходимо обновить аренду через сервер. Когда срок аренды истекает или удаляется с сервера, аренда становится неактивной.

Исключенный адрес

Исключенный адрес — это IP-адрес, который не назначается клиентам сервером DHCP.

Пул адресов

Пул адресов — это набор IP-адресов, которые DHCP-сервер может назначить клиентам.

Опция

Опция — это параметр, заданный сервером DHCP при обслуживании клиента DHCP при присвоении адреса. Например, общедоступный параметр включает в себя IP-адреса шлюза по умолчанию (маршрутизатора), WINS-сервера и DNS-сервера. DHCP-сервер позволяет настраивать другие параметры. Хотя большинство параметров определены в RFC 2132, можно добавить пользовательские параметры.

4.3.2. Обзор

Функция	Описание
Сервер DHCP	Включите сервер DHCP на устройстве, и он может динамически назначать IP-адреса и передавать конфигурации клиентам DHCP
Агент DHCP Relay агент	Включите функцию DHCP Relay на устройстве, и он может пересылать запросы DHCP и отвечать на пакеты в разных сегментах сети
Клиент DHCP	Включите DHCP-клиент на устройстве, и он может автоматически получать IP-адреса и конфигурации с DHCP-сервера

Функция	Описание
Правила AM	Включите правило AM на устройстве, и оно может назначать IP-адреса в соответствии с правилом

4.3.3. Сервер DHCP

4.3.3.1. Принцип работы

Принцип работы DHCP

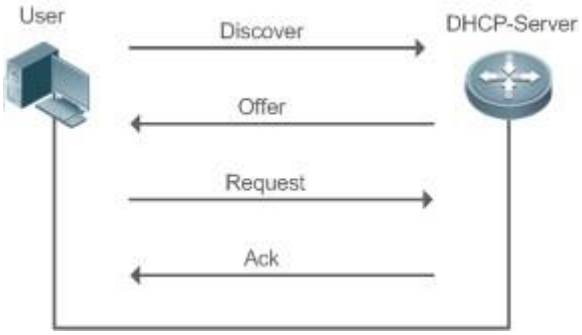


Рисунок 4-6.

Хост запрашивает IP-адрес через DHCP следующим образом:

1. Хост передает пакет обнаружения (discover) DHCP для поиска серверов DHCP в сети.
2. DHCP-сервер отправляет Broadcast/Unicast пакет (на основе пакета хоста). содержащий IP-адрес, MAC-адрес, имя домена и аренду (offer).
3. Хост передает пакет запросов DHCP для официального запроса IP-адреса (request).
4. DHCP-сервер отправляет на хост пакет DHCP ACK unitcast для подтверждения запроса.

ПРИМЕЧАНИЕ: DHCP-клиент может получать пакеты DHCP OFFER от нескольких серверов DHCP, но обычно он принимает только первый пакет DHCP OFFER. Кроме того, адрес, указанный в пакете DHCP OFFER, не обязательно назначается. Вместо этого он сохраняется сервером DHCP до тех пор, пока клиент не отправит формальный запрос.

Чтобы официально запросить IP-адрес, клиент передает пакет DHCP REQUEST, чтобы все DHCP-серверы, посылающие пакеты DHCP OFFER, могли получить пакет и освободить IP-адреса, предложенные в OFFER.

Если пакет DHCP OFFER содержит недопустимые параметры конфигурации, клиент отправляет на сервер пакет DHCP DECLINE, чтобы отклонить конфигурацию.

Если во время переговоров клиент не отвечает на пакеты DHCP OFFER вовремя, серверы отправят клиенту пакеты DHCP NAK, и клиент повторно инициирует процесс.

Во время построения сети серверы QTECH DHCP обладают следующими преимуществами:

- Упрощенная конфигурация. Динамическое назначение IP-адресов значительно упрощает настройку устройства.
- Централизованное управление. Конфигурацию нескольких подсетей можно изменить, просто изменив конфигурацию сервера DHCP.

Пул адресов

После того как сервер получает пакет запросов клиента, он выбирает допустимый пул адресов, определяет доступный IP-адрес из пула посредством PING и передает конфигурацию пула и адреса клиенту. Информация об аренде сохраняется локально для проверки действительности при возобновлении аренды.

Пул адресов может иметь следующие параметры конфигурации:

- Диапазон IP-адресов, который представляет собой диапазон доступных IP-адресов.
- Адрес шлюза. Поддерживается не более 8 адресов шлюзов.
- DNS-адрес. Поддерживается не более 8 адресов DNS.
- Срок аренды, уведомляющий клиентов о том, когда им нужно получить адрес и запросить продление срока аренды.

Контроль состояния VRRP

В сценарии протокола резервирования виртуального маршрутизатора (VRRP) устройства QTECH, поддерживающие DHCP, предоставляют команду для мониторинга состояния интерфейса VRRP. В интерфейсе, настроенном на использование адреса VRRP и мониторинга VRRP, DHCP-сервер обрабатывает только пакеты запросов DHCP-клиентов из интерфейса в режиме Master, а другие пакеты отбрасываются. Если адрес VRRP не настроен, DHCP-сервер не отслеживает состояние VRRP и все пакеты DHCP обрабатываются. Контроль состояния VRRP настраивается только на интерфейсах уровня 3. По умолчанию он отключен, а именно, только главное устройство обрабатывает службу DHCP.

Назначение IP-адреса на основе VLAN, портов и диапазона IP

После развертывания пула IP-адресов указанный диапазон IP-адресов назначается на основе сетей VLAN и портов. Существует три сценария:

1. Глобальная конфигурация.
2. Конфигурация на основе сетей VLAN, портов и диапазона IP-адресов.
3. Сочетание: 1 и 2. В сценарии 1 адреса назначаются глобально. В сценарии 2 адреса в указанном диапазоне IP назначаются только клиентам указанных сетей VLAN и портов. В сценарии 3 клиентам указанных сетей VLAN и портов назначаются адреса в указанном диапазоне IP, а другим клиентам — глобальные адреса по умолчанию.

4.3.3.2. Связанная конфигурация

Глобальное включение DHCP-сервера

- По умолчанию DHCP-сервер отключен.
- Запустите команду **service dhcp**, чтобы включить сервер DHCP.

Настройка пула адресов

- По умолчанию пул адресов не настроен.
- Выполните команду пула **ip dhcp pool**, чтобы настроить диапазон IP-адресов, шлюз и DNS.
- Если пул адресов не настроен, адреса не будут назначены.

4.3.4. Агент DHCP Relay

4.3.4.1. Принцип работы

IP-адрес назначения пакетов запросов DHCP — 255.255.255.255, и эти пакеты пересылаются в подсети. Для назначения IP-адреса по сегментам сети необходим агент ретрансляции DHCP. Агент ретрансляции DHCP передает пакеты запросов DHCP серверу DHCP и пересылает пакеты ответа DHCP клиенту DCHP. Агент DHCP Relay служит ретранслятором, подключаемым к клиенту DHCP и серверу DHCP различных сегментов сети, путем пересылки пакетов запросов DHCP и пакетов ответа DHCP. В режиме Client-Relay-Server управление IP-адресами в нескольких сегментах сети осуществляется только одним DHCP-сервером. См. рисунок ниже.

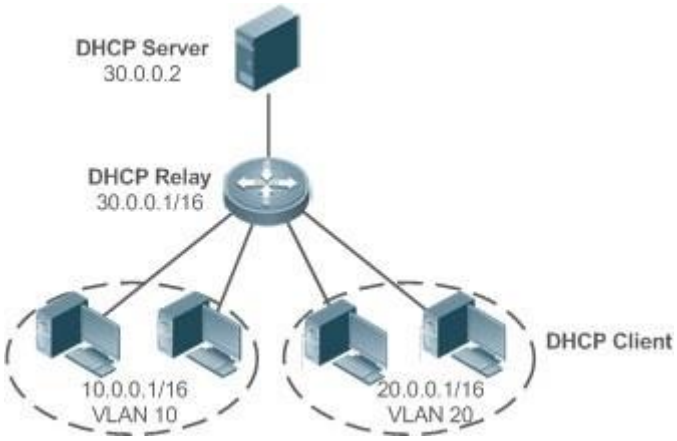


Рисунок 4-7. Сценарий DHCP Relay

VLAN 10 и VLAN 20 соответствуют сегментам 10.0.0.1/16 и 20.0.0.1/16 соответственно. Сервер DHCP с IP-адресом 30.0.0.2 находится в сегменте 30.0.0.1/16. Для управления динамическими IP-адресами в сетях VLAN 10 и VLAN 20 сервером DHCP необходимо включить ретрансляции DHCP на шлюзе и настроить IP-адрес 30.0.0.2 для сервера DHCP.

Информация о ретрансляторе DHCP (опция 82)

Как определено в RFC3046, можно добавить параметр для указания сетевой информации клиента DHCP при выполнении DHCP Relay, чтобы сервер DHCP мог назначать IP-адреса различных привилегий на основе более точной информации. Этот параметр называется опция 82. В настоящее время устройства QTECH поддерживают четыре схемы информации о релейных агентах, которые описаны соответственно следующим образом:

1. Опция информации о dot1x: Эта схема должна быть реализована с аутентификацией 802.1X. Агент ретрансляции DHCP формирует подопцию идентификатора цепи на основе привилегий IP и идентификатора VLAN клиента DHCP. Формат параметра показан на следующем Рисунке.

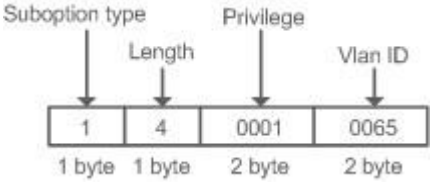


Рисунок 4-8. Формат параметра

2. Информация агента ретрансляции в опции 82: Эта схема служит без корреляции с другими модулями протоколов. Агент DHCP Relay формирует опцию 82 на основе физического порта, получающего пакеты запросов DHCP, и MAC-адреса устройства. Формат параметра показан на следующем Рисунке.

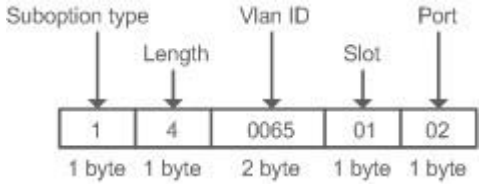


Рисунок 4-9. Идентификатор цепи агента

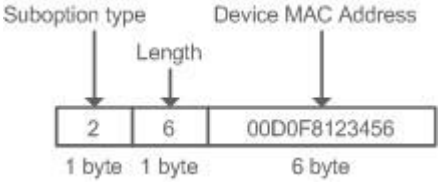


Рисунок 4-10. Удаленный идентификатор оператора

3. Опция информации о ретрансляторе VPN: Эта схема должна быть реализована с функционалом MPLS VPN.

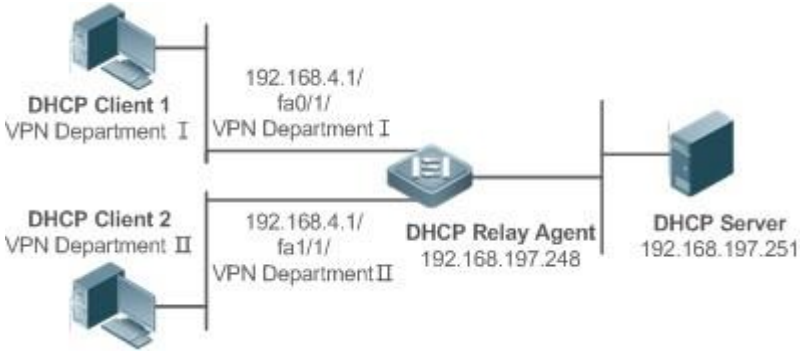


Рисунок 4-11. Приложение в среде MPLS VPN

Как показано на Рисунке 4-11, в среде MPLS VPN клиент DHCP 1 подключен к fa0/1 через relay агента DHCP и DHCP Client 2 на fa1/1. Интерфейсы fa0/1 и fa1/1 относятся к разным VRFs. DHCP Client 1 и DHCP Client 2 получают IP-адреса через DHCP. Согласно планированию сети, VPN Department I и VPN Department II находятся в одном сегменте 192.168.4.0/24. В этом случае обычное приложение DHCP не может удовлетворить потребности. Для поддержки ретрансляции DHCP в среде MPLS VPN вводится **option vpn**, которая включает три подпараметра, а именно VPN-ID, Subnet-Selection и Server-Identifier-Override.

- VPN-ID: когда агент ретрансляции DHCP получает пакет запроса DHCP, он добавляет информацию о VPN, которую клиент DHCP находит в пакете, в качестве опции. DHCP-сервер сохраняет VPN-ID в ответном пакете, а агент ретрансляции DHCP пересылает пакет на соответствующий VRF в соответствии с опцией. Формат параметра показан на следующем Рисунке.

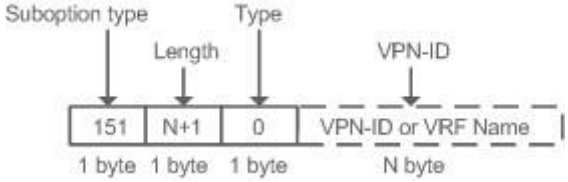


Рисунок 4-12. VPN-ID

- Subnet-Selection: в конвенциональной ретрансляции DHCP информация о клиентской сети и адреса сервера DHCP и агента ретрансляции DHCP указывается в поле **gateway address [giaddr]**. В среде MPLS VPN задайте **giaddr**

на IP-адрес интерфейса агента DHCP Relay, подключенного к серверу DHCP, чтобы сервер мог напрямую взаимодействовать с агентом Relay. Кроме того, информация о подсети клиента указывается в параметре Subnet-Selection (Выбор подсети). Формат параметра показан на следующем Рисунке.

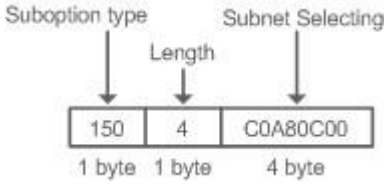


Рисунок 4-13. Выбор подсети

- Server-Identifier-Override: в среде MPLS VPN пакеты запросов от клиента DHCP не могут быть отправлены напрямую на сервер DHCP. Агент DHCP Relay использует эту опцию для передачи информации интерфейса, связывающий агент ретрансляции и сервер DHCP. Когда сервер отправляет ответное сообщение, этот параметр переопределяет параметр Server-Identifier. Таким образом, клиент DHCP отправляет пакеты агенту ретрансляции DHCP, а агент ретрансляции DHCP пересылает их на сервер DHCP. Формат параметра показан на следующем Рисунке.

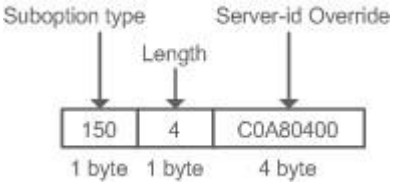


Рисунок 4-14. Server-Identifier-Override

Идентификатор сервера проверки DHCP Relay

В среде DHCP для сети развертывается несколько серверов DHCP, что обеспечивает резервирование сервера для обеспечения бесперебойной работы сети. После включения этой функции пакет запроса DHCP, отправленный клиентом, содержит параметр идентификатора сервера, указывающий сервер DHCP. Чтобы облегчить нагрузку на серверы в определенных средах, необходимо включить эту функцию на Relay агенте, для отправки пакета на указанный сервер DHCP, а не на все серверы DHCP.

Подавление ретрансляции DHCP

После настройки команды IP DHCP Relay Suppression на интерфейсе пакеты запросов DHCP, полученные на интерфейсе, будут отфильтрованы, а другие пакеты запросов DHCP будут пересылаться.

4.3.4.2. Связанная конфигурация

Включение ретрансляции DHCP

- По умолчанию функция DHCP Relay отключена.
- Для включения ретрансляции DHCP можно выполнить команду **service dhcp**.
- Перед началом работы необходимо включить DHCP Relay.

Настройка IP-адреса для сервера DHCP

- По умолчанию для сервера DHCP не задан отслеживаемый IP-адрес.
- Можно выполнить команду **ip helper-address** для настройки IP-адреса для сервера DHCP. IP-адрес можно настроить глобально или через интерфейс уровня 3. Можно настроить не более 20 IP-адресов DHCP-сервера.

- Когда интерфейс получает пакет запросов DHCP, конфигурация сервера DHCP на интерфейсе преобладает над конфигурацией, настроенной глобально. Если на интерфейсе не настроен адрес DHCP-сервера, будет использоваться глобально настроенный DHCP сервер.

Включение опции DHCP 82

- По умолчанию опция DHCP 82 отключена.
- Для включения опции DHCP 82 можно запустить команду **ip dhcp relay information option82**.

Включение DHCP Relay Check Server-ID

- По умолчанию идентификатор сервера проверки ретрансляции DHCP отключен.
- Можно запустить команду **ip dhcp relay check server-id**, чтобы включить DHCP Relay Check Server-id

Включение подавления ретрансляции DHCP

- По умолчанию функция подавления ретрансляции DHCP отключена на всех интерфейсах.
- Можно запустить команду **ip dhcp relay suppression**, чтобы включить ее в интерфейсе.

4.3.5. Клиент DHCP

4.3.5.1. Принцип работы

DHCP-клиент передает пакет обнаружения DHCP после входа в состояние Init. Затем он может получить несколько пакетов предложений DHCP. Он выбирает один из них и отвечает на соответствующий DHCP-сервер. После этого он отправляет пакеты запроса на продление аренды в процессы возобновления и повторной привязки периода старения для запроса на продление аренды.

4.3.5.2. Связанная конфигурация

Включение клиента DHCP в интерфейсе

- По умолчанию клиент DHCP отключен.
- В режиме настройки интерфейса можно запустить команду **ip address dhcp**, чтобы включить DHCP Client.
- Чтобы включить службу DHCP, необходимо включить DHCP Client.
- Конфигурация используется на интерфейсе уровня 3, например, на SVI или маршрутизируемых портах.

4.3.6. Правила AM

4.3.6.1. Принцип работы

Правило AM определяет диапазон IP-адресов, назначенных клиентам DHCP в различных сетях VLAN и портах. Его можно использовать для быстрой идентификации VLAN и порта неисправного клиента DHCP и эффективного назначения адресов. После настройки правила AM все клиенты DHCP из заданной VLAN и порты могут получать IP-адреса. Если правило AM не настроено, существует два следующих случая: если задано правило AM по умолчанию, клиент получает IP-адрес из диапазона по умолчанию; если правило AM по умолчанию не настроено, клиент не сможет получить IP-адрес.

4.3.6.2. Связанная конфигурация

Настройка правила AM в режиме глобальной конфигурации

- В режиме глобальной конфигурации выполните команду **address-manage**, чтобы войти в режим конфигурации правил AM.
- Выполните команду **match ip default**, чтобы настроить правило AM по умолчанию.
- Выполните команду **match ip**, чтобы настроить правило AM на основе VLAN и порта или порта в отдельности.

4.4. Настройка

4.4.1. Настройка сервера DHCP

Настройка	Описание и команда	
Настройка динамического IP-адреса	(Обязательно) Используется для включения DHCP-сервера для динамического назначения IP-адреса	
	service dhcp	Включает DHCP-сервер
	ip dhcp pool	Настройка пула адресов
	network	Настройка номера сети и маски подсети пула адресов DHCP
	(Необязательно) Используется для настройки свойств пула адресов	
	default-router	Настройка шлюза клиента по умолчанию
	lease	Настройка аренды адреса
	next-server	Настройка адреса TFTP-сервера
	bootfile	Настройка загрузочного файла клиента
	domain-name	Настройка доменного имени клиента
	dns-server	Настройка сервера доменных имен

Настройка	Описание и команда	
Настройка динамического IP-адреса	**netbios-name-server**	Настройка WINS-сервера NetBIOS
	netbios-node-type	Настройка типа узла NetBIOS на клиенте
	lease-threshold	Настройка порога срабатывания сигнализации для пула адресов
	option	Настройка параметра, заданного пользователем
	pool-status	Включение или отключение пула адресов
Настройка статического IP-адреса	(Необязательно) Используется для статического назначения IP-адреса клиенту	
	ip dhcp pool	Настройка имени пула адресов и переход в режим конфигурации пула адресов
	host	Настройка IP-адреса и маски подсети хоста клиента
	hardware-address	Настройка аппаратного адреса клиента
	client-identifier	Настройка уникального идентификатора клиента
	client-name	Настройка имени клиента
Настройка правила AM для сервера DHCP	(Необязательно) он используется для настройки свойств DHCP-сервера	
	ip dhcp excluded-address	Настройка исключенного IP-адреса
	ip dhcp force-send-nak	Настройка обязательного ответа NAK сервером DHCP
	ip dhcp monitor-vrrpstate	Настройка мониторинга состояния VRRP

Настройка	Описание и команда	
Настройка правила AM для сервера DHCP	**ip dhcp ping packets**	Настройка времени эхо-запроса
	ip dhcp ping timeout	Настройка тайм-аута ping
	ip dhcp server arpdetect	Настройка DHCP-сервера для обнаружения пользователя в автономном режиме
Настройка глобальных свойств DHCP-сервера	(Необязательно) он используется для настройки правила AM сервера DHCP	
	match ip default	Настройка правила AM по умолчанию
	match ip ip-address	Настройка правила AM на основе VLAN и порта

4.4.2. Настройка DHCP-ретрансляции

Настройка	Описание и команда	
Настройка основных функций DHCP	(Обязательно) используется для включения ретрансляции DHCP	
	service dhcp	Включение ретрансляции DHCP
	ip helper-address	Настройка IP-адреса сервера DHCP
Настройка DHCP Relay опции 82	(Необязательно) он используется для назначения клиентам IP-адресов с разными привилегиями в сочетании с информацией о физическом порте. Эту функцию нельзя использовать вместе с командой **dhcp option dot1x**	
	ip dhcp relay information option82	Включение опции DHCP 82

Настройка	Описание и команда	
Настройка проверки Server ID для DHCP Relay	(Необязательно) он используется для того, чтобы агент DHCP Relay посылала пакеты запросов DHCP только на указанный сервер	
	ip dhcp relay check server-id	Позволяет агенту ретрансляции DHCP отправлять пакеты запросов DHCP только на указанный сервер
Настройка подавления DHCP	(Необязательно) он используется для защиты пакетов запросов DHCP на интерфейсе	
	ip dhcp relay suppression	Включает подавление ретрансляции DHCP

4.4.3. Настройка клиента DHCP

Настройка	Описание и команда	
Настройка клиента DHCP	(Обязательно) он используется для включения клиента DHCP	
	ip address dhcp	Обеспечивает интерфейс Ethernet, инкапсулированный интерфейс PPP/HDLC или FR-инкапсулированный интерфейс для получения IP-адресов через DHCP

4.4.4. Настройка динамического IP-адреса

4.4.4.1. Результат конфигурации

Предоставление всем клиентам DHCP услуг DHCP, включая назначение IP-адресов и шлюзов.

4.4.4.2. Примечания

DHCP-сервер и ретрансляция DHCP совместно используют служебную команду **service dhcp**, но устройство не может одновременно работать как DHCP-сервер и ретранслятор. Если устройство настроено с допустимым пулом адресов, оно действует как сервер и пересылает пакеты. В противном случае он служит в качестве relay-агента.

4.4.4.3. Этапы конфигурации

Включение DHCP-сервера

- Обязательно. Он обеспечивает динамическое назначение IP-адресов.
- Запустите команду **service dhcp** в режиме глобальной конфигурации.

Настройка пула адресов

- Обязательно. Он используется для создания пула IP-адресов.
- Запустите команду пула **ip dhcp pool** в режиме глобальной конфигурации.

Настройка сетевого номера и маски подсети пула адресов DHCP

- Обязательно. Он определяет диапазон динамически назначаемых адресов.
- Выполните команду **network** в режиме конфигурации пула адресов DHCP.

Настройка шлюза клиента по умолчанию

- Опционально. Он используется для настройки адреса шлюза.
- Запустите команду **default-router** в режиме конфигурации пула адресов DHCP.

Настройка аренды адреса

- Опционально. Он используется для настройки аренды IP-адреса, которая по умолчанию составляет 24 часа.
- Выполните команду **lease** аренды в режиме конфигурации пула адресов DHCP.

Настройка адреса TFTP-сервера

- Опционально. Он используется для настройки адреса TFTP-сервера.
- Выполните команду **next-server** в режиме конфигурации пула адресов DHCP.

Настройка доменного имени клиента

- Опционально. Он используется для настройки доменного имени клиента.
- Выполните команду **domain-name** в режиме конфигурации пула адресов DHCP.

Настройка DNS

- Опционально. Он используется для настройки адреса DNS.
- Выполните команду **dns** в режиме конфигурации пула адресов DHCP.

Настройка WINS-сервера NetBIOS

- Опционально. Он используется для настройки адреса WINS-сервера NetBIOS.
- Запустите команду **netbios-name-server** в режиме конфигурации пула адресов DHCP.

Настройка типа узла NetBIOS на клиенте

- Опционально. Он используется для настройки типа узла NetBIOS.
- Запустите команду **netbios-name-type** в режиме конфигурации пула адресов DHCP.

Настройка порога аварийного сигнала для пула адресов

- Опционально. Он используется для управления количеством лизинговых соглашений. При достижении порогового значения (90 % по умолчанию) будет распечатан сигнал тревоги.
- Выполните команду **lease-threshold** в режиме конфигурации пула адресов DHCP.

Настройка параметра, заданного пользователем

- Опционально. Он используется для настройки пользовательских параметров.
- Выполните команду **option** в режиме конфигурации пула адресов DHCP.

Включение или отключение пула адресов

- Опционально. Он используется для включения или отключения пула адресов. По умолчанию данная функция включена.
- Выполните команду **pool-status** в режиме конфигурации пула адресов DHCP.

4.4.4.4. Проверка конфигурации

Подключение клиента DHCP и сервера DHCP.

- Проверьте, получает ли клиент конфигурации на сервере.

4.4.4.5. Связанные команды

Включение DHCP-сервера

Команда	**service dhcp**
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Включите сервер DHCP и ретрансляцию DHCP. DHCP-сервер и ретрансляцию DHCP совместно используют служебную команду **service dhcp**. Если устройство настроено с допустимым пулом адресов, оно действует как сервер и пересылает пакеты. В противном случае он служит в качестве релейного агента

Настройка пула адресов

Команда	**ip dhcp pool** *dhcp-pool*
Описание параметров	*pool-name*: указывает имя пула адресов
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Перед назначением IP-адреса клиенту необходимо настроить имя пула адресов и войти в режим конфигурации пула адресов DHCP

Настройка сетевого номера и маски подсети пула адресов DHCP

Команда	**network** network-number mask [low-ip-address high-ip-address]
Описание параметров	*network-number:* указывает номер сети пула IP-адресов. *mask:* указывает маску подсети пула IP-адресов. Если маска подсети не определена, применяется естественная маска подсети
Режим конфигурации	Режим конфигурации пула адресов DHCP

Встроенная подсказка	Для настройки динамического назначения адресов необходимо настроить сетевой идентификатор и маску подсети для пула адресов, чтобы предоставить серверу DHCP диапазон адресов. IP-адреса в пуле назначаются в указанном порядке. Если адрес назначен или существует в целевом сегменте сети, следующий адрес будет проверяться до тех пор, пока не будет назначен действительный адрес. Беспроводное оборудование QTECH предоставляет доступные сегменты сети, указывая начальный и конечный адреса. Конфигурация не является дополнительной. Если начальный и конечный адреса не указаны, будут назначаться все IP-адреса в сегменте сети. Для оборудования QTECH адреса назначаются на основе физического адреса и идентификатора клиента. Таким образом, одному клиенту не будет назначено две аренды из одного пула адресов. В случае топологической избыточности между клиентом и сервером назначение адреса может быть не выполнено. Чтобы избежать таких сбоев, администратору сети необходимо предотвратить избыточность путей в построении сети, например, путем настройки физических каналов или сетевых путей

Настройка шлюза клиента по умолчанию

Команда	**default-router** address [address2…address8]
Описание параметров	*address*: указывает IP-адрес шлюза по умолчанию. Настройте хотя бы один IP-адрес. *ip-address2…ip-address8:* (ОПЦИОНАЛЬНО) можно настроить не более 8 шлюзов
Режим конфигурации	Режим конфигурации пула адресов DHCP
Встроенная подсказка	Настройте шлюз клиента по умолчанию, и сервер будет предоставлять конфигурацию шлюза к клиенту. IP-адреса шлюза по умолчанию и клиента должны находиться в одной сети

Настройка аренды адреса

Команда	**lease** {*days* [*hours]* [*minutes*] | **infinite**}
Описание параметров	*days:* определяет аренду в днях. hours: (Необязательно) определяет аренду в часах. Определите дни до часов. minutes: (Необязательно) определяет срок аренды в минутах. Определите дни и часы до минут. **infinite:** определение неограниченной аренды

Режим конфигурации	Режим конфигурации пула адресов DHCP
Встроенная подсказка	Аренда IP-адреса по умолчанию, назначенного сервером DHCP, составляет 1 день. Когда срок аренды истекает в ближайшее время, клиенту необходимо запросить продление аренды. В противном случае IP-адрес не может быть использован после истечения срока аренды

Настройка загрузочного файла на клиенте

Команда	**bootfile** *filename*
Описание параметров	*file-name*: определяет имя загрузочного файла
Режим конфигурации	Режим конфигурации пула адресов DHCP
Встроенная подсказка	Загрузочный файл — это загрузочный файл образа, используемый при запуске клиента. Обычно файл является ОС, загруженной клиентом DHCP

Настройка доменного имени клиента

Команда	**domain-name** *domain*
Описание параметров	*domain-name:* определяет доменное имя клиента DHCP
Режим конфигурации	Режим конфигурации пула адресов DHCP
Встроенная подсказка	Можно задать имя домена для клиента. Когда клиент получает доступ к сети через имя хоста, имя домена добавляется автоматически для завершения имени хоста

Настройка DNS

Команда	**dns-server** { *ip-address* [*ip-address2…ip-address8*]
Описание параметров	*ip-address:* определяет IP-адрес DNS-сервера. Настройте хотя бы один IP-адрес. *ip-address2…ip-address8:* (ОПЦИОНАЛЬНО) можно настроить не более 8 DNS-серверов
Режим конфигурации	Режим конфигурации пула адресов DHCP

Встроенная подсказка	Если клиент получает доступ к сетевым ресурсам через имя домена, необходимо настроить DNS-сервер для разрешения имени домена

Настройка WINS-сервера NetBIOS

Команда	**netbios-name-server** *address* [*address2…address8*]
Описание параметров	*address:* определяет IP-адрес WINS-сервера. Настройте хотя бы один IP-адрес. *ip-address2…ip-address8:* (ОПЦИОНАЛЬНО) можно настроить не более 8 WINS-серверов
Режим конфигурации	Режим конфигурации пула адресов DHCP
Встроенная подсказка	WINS — это служба доменных имен, с помощью которой сеть Microsoft TCP/IP разрешает имя NetNBIOS на IP-адрес. Сервер WINS — это сервер Windows NT. При запуске WINS-сервера он получает запрос на регистрацию от WINS-клиента. Когда клиент выключается, он отправляет сообщение об освобождении имени, чтобы компьютеры в базе данных WINS и в сети были согласованными

Настройка типа узла NetBIOS на клиенте

Команда	**netbios-node-type** *type*
Описание параметров	*type*: определяет тип узла NetBIOS с помощью одного из следующих подходов. 1. Шестнадцатеричное число от 0 до FF. Доступны только следующие значения. • b-node • p-node • m-node • 8 для h-node 2. Символьная строка. • b-node для широковещательного узла • p-node для одноранговой узла • m-node для смешанного узла • h-node для гибридного режима
Режим конфигурации	Режим конфигурации пула адресов DHCP

Встроенная подсказка	Существует четыре типа узлов NetBIOS клиента Microsoft DHCP. 1. Широковещательный узел. Для такого узла разрешение имен NetBIOS запрашивается через широковещательную рассылку. 2. Узел одноранговой сети. Клиент отправляет запрос на разрешение на WINS-сервер. 3. Смешанный узел. Клиент передает запрос на разрешение и отправляет запрос на разрешение на WINS-сервер. 4. Гибридный узел. Клиент отправляет запрос на разрешение на WINS-сервер. Если ответ не получен, клиент будет передавать запрос на разрешение. По умолчанию операционная система Microsoft является широковещательным или гибридным узлом. Если сервер WINS не настроен, это широковещательный узел. В противном случае это гибридный узел

Настройка параметра, заданного пользователем

Команда	**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }
Описание параметров	*code:* определяет код опции DHCP. **ascii** *string:* определяет строку символов ASCII. **hex** *string:* определяет шестнадцатеричную символьную строку. **ip** *ip-address:* определяет IP-адрес
Режим конфигурации	Режим конфигурации пула адресов DHCP
Встроенная подсказка	DHCP позволяет передавать информацию о конфигурации хосту по сети TCP/IP. Пакеты DHCP содержат поле параметра, определяемого содержимого. DHCP-клиент должен иметь возможность получать пакет DHCP с возможностью переноса не менее 312 байт. Кроме того, фиксированное поле данных в пакете DHCP также называется опцией. В беспроводной локальной сети клиент DHCP точки доступа динамически запрашивает IP-адрес сети переменного тока. На сервере DHCP можно настроить команду **option**, указав адрес AC

Включение или отключение пула адресов

Команда	**pool-status** {**enable | disable**}
Описание параметров	**enable***:* включение пула адресов. **disable***:* отключение пула адресов. По умолчанию данная функция включена
Режим конфигурации	Режим конфигурации пула адресов DHCP

Встроенная подсказка	Оборудование QTECH предоставляет команду для включения/отключения пула адресов DHCP

4.4.4.6. Пример конфигурации

Настройка пула адресов

Этапы конфигурации	• Определите сеть пула адресов. • Сегмент сети 172.16.1.0/24. • Шлюз по умолчанию — 172.16.1.254. • Аренда адреса — 1 день. • Диапазон исключенных адресов от 172.16.1.2 до 172.16.1.100
	QTECH(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100 QTECH(dhcp-config)# ip dhcp pool net172 QTECH(dhcp-config)# network 172.16.1.0 255.255.255.0 QTECH(dhcp-config)# default-router 172.16.1.254 QTECH(dhcp-config)# lease 1
Проверка конфигурации	• Выполните команду **show run** для отображения конфигурации
	QTECH(config)#show run | begin ip dhcp ip dhcp excluded-address 172.16.1.2 172.16.1.100 ip dhcp pool net172 network 172.16.1.0 255.255.255.0 default-router 172.16.1.254 lease 1

4.4.5. Настройка статического IP-адреса

4.4.5.1. Результат конфигурации

Назначьте конкретные IP-адреса и конфигурацию определенным клиентам DHCP.

4.4.5.2. Этапы конфигурации

Настройка имени пула адресов и переход в режим конфигурации пула адресов

- Обязательно. Он используется для создания пула IP-адресов.
- Запустите команду пула **ip dhcp pool** в режиме глобальной конфигурации.

Настройка IP-адреса и маски подсети клиента

- Обязательно. Он используется для настройки статического IP-адреса и маски подсети.
- Выполните команду **host** в режиме конфигурации пула адресов DHCP.

Настройка аппаратного адреса клиента

- Опционально. Он используется для настройки адреса MAC.
- Выполните аппаратную команду **hardware** в режиме конфигурации пула адресов DHCP.

Настройка уникального идентификатора клиента

- Опционально. Он используется для настройки статического идентификатора пользователя (UID).
- Запустите команду **client-identifier** в режиме конфигурации пула адресов DHCP.

Настройка имени клиента

- Опционально. Он используется для настройки статического имени клиента.
- Запустите команду **host-name** в режиме конфигурации пула адресов DHCP.

4.4.5.3. Проверка конфигурации

Проверьте, получает ли клиент IP-адрес, когда он находится в оперативном режиме.

4.4.5.4. Связанные команды

Настройка пула адресов

Команда	**ip dhcp pool** *dhcp-pool*
Описание параметров	*pool-name*: указывает имя пула адресов
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Перед назначением IP-адреса клиенту необходимо настроить имя пула адресов и войти в режим конфигурации пула адресов

Привязка IP-адреса вручную

Команда	**host** *ip-address* [*netmask*] **client-identifier** *unique-identifier* **client-name** *name*
Описание параметров	*ip-address:* определяет IP-адрес клиента DHCP. *netmask:* определяет маску подсети клиента DHCP. *unique-identifier:* определяет аппаратный MAC-адрес (например, aabb.bbbb.bb88) и идентификатор (например, 01aa.bbbb.bbbb.88) клиента DHCP. *name:* (Необязательно) определяет имя клиента, используя символы ASCII. Имя не включает имя домена. Например, назовите хост **mary**, а не **mary.qtech.ru**

Режим конфигурации	Режим конфигурации пула адресов DHCP
Встроенная подсказка	Привязка адреса означает сопоставление IP-адреса и MAC-адреса клиента. Существует два вида привязки адресов. 1. Статическая привязка. Привязка вручную может рассматриваться как специальный пул адресов DHCP с одним адресом. 2. Динамическое привязка. DHCP-сервер динамически назначает клиенту IP-адрес из пула при получении запроса DHCP, создавая связь между IP-адресом и MAC-адресом клиента. Чтобы настроить привязку вручную, необходимо определить пул хостов, а затем указать IP-адрес и аппаратный адрес или идентификатор клиента DHCP. Аппаратный адрес — это MAC-адрес. Идентификатор клиента включает тип сетевого носителя и MAC-адрес. Клиент Microsoft обычно идентифицируется по идентификатору клиента, а не по MAC-адресу. Коды типов сред см. в разделе Параметры протокола разрешения адресов (*Address Resolution Protocol Parameters*) в RFC 1700. Код типа Ethernet-станции **01**

4.4.5.5. Пример конфигурации

Динамический пул IP-адресов

Этапы конфигурации	• Настройте пул адресов VLAN 1 с IP-адресом 20.1.1.0 и маской подсети 255.255.255.0 • Шлюз по умолчанию — 20.1.1.1 • Время аренды — 1 день
	QTECH(config)# ip dhcp pool vlan1 QTECH(dhcp-config)# network 20.1.1.0 255.255.255.0 QTECH(dhcp-config)# default-router 20.1.1.1 QTECH(dhcp-config)# lease 1 0 0
Проверка конфигурации	Выполните команду **show run** для отображения конфигурации
	QTECH(config)#show run | begin ip dhcp ip dhcp pool vlan1 network 20.1.1.0 255.255.255.0 default-router 20.1.1.1 lease 1 0 0

Привязка (lease) статистически

Этапы конфигурации	• Адрес хоста — 172.16.1.101, а маска подсети — 255.255.255.0. • Имя хоста — Ivan.qtech.ru • Шлюз по умолчанию — 172.16.1.254 • Mac-адрес: 00d0.df34.32a3
	QTECH(config)# ip dhcp pool Ivan QTECH(dhcp-config)# host 172.16.1.101 255.255.255.0 QTECH(dhcp-config)# client-name Ivan QTECH(dhcp-config)# hardware-address 00d0.df34.32a3 Ethernet QTECH(dhcp-config)# default-router 172.16.1.254
Проверка конфигурации	• Выполните команду **show run** для отображения конфигурации
	QTECH(config)#show run | begin ip dhcp ip dhcp pool Ivan host 172.16.1.101 255.255.255.0 client-name Ivan hardware-address 00d0.df34.32a3 Ethernet default-router 172.16.1.254

4.4.6. Настройка правила AM для сервера DHCP

4.4.6.1. Результат конфигурации

Назначьте IP-адреса в соответствии с правилом AM на основе порта и VLAN.

4.4.6.2. Примечания

Оборудование QTECH поддерживает конфигурацию правил AM на интерфейсах Ethernet, GB, FR, PPP и HDLC.

4.4.6.3. Этапы конфигурации

Настройка управления адресами

- Обязательно. Войдите в режим управления адресами.
- Запустите команду **address-manage** в режиме настройки управления адресами.

Настройка правила AM

- Обязательно. Настройте правило AM на основе порта и VLAN.
- Выполните команду **match ip** в режиме настройки управления адресами.

4.4.6.4. Проверка конфигурации

Проверьте, получают ли клиенты в разных сетях VLAN и портах действительные IP-адреса.

4.4.6.5. Связанные команды

Настройка диапазона по умолчанию

Команда	**match ip default** *ip-address netmask*
Описание параметров	*ip-address:* определяет IP-адрес. *netmask:* определение маски подсети
Режим конфигурации	Режим управления адресами
Встроенная подсказка	После настройки всем клиентам DHCP назначаются IP-адреса из диапазона по умолчанию на основе VLAN и порта. Если эта команда не настроена, IP-адреса будут назначаться обычным образом

Назначение динамического IP-адреса на основе VLAN и порта

Команда	**match ip** *ip-address netmask interface* [**add**/**remove**] **vlan** *vlan-list*
Описание параметров	*ip-address:* определяет IP-адрес. *netmask:* определение маски подсети. *interface:* определяет имя интерфейса. *add/remove:* добавление или удаление определенной VLAN. *vlan-list:* указывает индекс VLAN
Режим конфигурации	Режим управления адресами
Встроенная подсказка	После настройки клиентам DHCP назначаются IP-адреса из диапазона адресов по умолчанию на основе VLAN и порта

Назначение статического IP-адреса на основе VLAN

Команда	**match ip** *ip-address netmask* [**add**/**remove**] **vlan** *vlan-list*
Описание параметров	*ip-address:* определяет IP-адрес. *netmask:* определение маски подсети. *add/remove:* добавление или удаление определенной VLAN. *vlan-list:* указывает индекс VLAN
Режим конфигурации	Режим управления адресами

Встроенная подсказка	В Super VLAN клиенту может быть назначен фиксированный статический адрес независимо от того, в какой Super VLAN находится клиент. Не нужно настраивать правило AM для этого IP-адреса на основе всех подсетей VLAN и портов, а только настраивать правило AM на основе VLAN. Это правило действует только для назначения статического адреса

4.4.6.6. Пример конфигурации

Настройка правила AM

Этапы конфигурации	• Настройте правило по умолчанию. • Настройте правило на основе определенной VLAN + порт + диапазон адресов. • Настройте правило на основе определенного диапазона VLAN-адресов
	QTECH(config)# address-manage QTECH(config-address-manage)# match ip default 172.50.128.0 255.255.128.0 QTECH(config-address-manage)# match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005 QTECH(config-address-manage)# match ip 10.1.6.0 255.255.255.0 vlan 1006
Проверка конфигурации	• Выполните команду **show run** для отображения конфигурации
	address-manage match ip default 172.50.128.0 255.255.128.0 match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005 match ip 10.1.6.0 255.255.255.0 vlan 1006

4.4.7. Настройка глобальных свойств DHCP-сервера

4.4.7.1. Результат конфигурации

Включите сервер с определенными функциями, например, ping и принудительный NAK.

4.4.7.2. Примечания

Настройка команды может привести к исключениям на других серверах.

4.4.7.3. Этапы конфигурации

Настройка исключенного IP-адреса

- Опционально. Настройте некоторые адреса или диапазоны адресов как недоступные.

- Запустите команду **ip dhcp excluded-address** в режиме глобальной конфигурации.

Настройка обязательного ответа NAK

- Опционально. Сервер отвечает на неверный запрос адреса с пакетом NAK.
- Запустите команду **ip dhcp force-send-nak** в режиме глобальной конфигурации.

Настройка мониторинга состояния VRRP

- Опционально. После настройки пакеты DHCP обрабатываются главным сервером.
- Запустите команду **ip dhcp monitor-vrrp-state** в режиме глобальной конфигурации.

Настройка времени пинга

- Опционально. Проверьте доступность адреса с помощью команды **ping**. По умолчанию: 2.
- Выполните команду **ip dhcp ping packet** в режиме глобальной конфигурации.

Настройка тайм-аута Ping

- Опционально. Проверьте доступность адреса с помощью команды **ping**. По умолчанию установлено значение 500 мс.
- Запустите команду **ip dhcp ping timeout** в режиме глобальной конфигурации.

Детектирование автономного обнаружения пользователя

- Настройте DHCP-сервер, чтобы определить, отключен ли клиент. Если клиент не подключается к сети в течение определенного периода времени, то будет получен адрес, назначенный клиенту.
- Запустите команду **ip dhcp server arp-detect** в режиме глобальной конфигурации.

4.4.7.4. Проверка конфигурации

Запустите команду **dhcp-server** и проверьте конфигурацию во время назначения адреса.

4.4.7.5. Связанные команды

Настройка исключенного IP-адреса

Команда	**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
Описание параметров	*low-ip-address:* указывает начальный IP-адрес. *high-ip-address:* указывает конечный IP-адрес
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Если не указано иное, DHCP-сервер назначает все адреса из пула IP-адресов клиентам DHCP. Чтобы зарезервировать некоторые адреса (например, адреса, уже назначенные серверу или устройствам), необходимо настроить эти адреса как исключенные. Для настройки DHCP-сервера рекомендуется настроить исключенные адреса, чтобы избежать конфликта адресов и сократить время обнаружения во время назначения адресов

Настройка обязательного ответа NAK

Команда	**ip dhcp force-send-nak**
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	В WLAN DHCP-клиент часто перемещается из одной сети в другую. Когда DHCP-сервер получает запрос на продление аренды от клиента, но обнаруживает, что клиент пересекает сетевой сегмент или срок аренды истек, он отправляет пакет NAK, чтобы потребовать от клиента получение IP-адреса снова. Это предотвращает постоянную отправку клиентом пакетов запросов до повторного получения IP-адреса после истечения времени ожидания. Сервер отправляет пакет NAK только при обнаружении записи аренды клиента. Когда DHCP-клиент пересекает сеть, DHCP-сервер не может найти запись аренды клиента и не будет отвечать пакетом NAK. Клиент постоянно отправляет пакеты запросов, прежде чем снова получить IP-адрес после истечения времени ожидания. Следовательно, получение IP-адреса занимает много времени. Это также происходит, когда сервер DHCP теряет аренду после перезапуска и клиент запрашивает продление аренды. В этом случае можно настроить команду, чтобы сервер DHCP мог ответить пакетом NAK, даже если он не может найти запись аренды, чтобы клиент мог быстро получить IP-адрес. Обратите внимание, что команда по умолчанию отключена. Чтобы включить его, в широковещательном домене можно настроить только один сервер DHCP

Настройка времени пинга

Команда	**ip dhcp ping packets** [*number*]
Описание параметров	*number:* (ОПЦИОНАЛЬНО) диапазоны от 0 до 10. 0 указывает на то, что функция ping отключена. По умолчанию используется два эхо-запроса
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	По умолчанию, когда DHCP-сервер назначает IP-адрес из пула, он дважды запускает команду Ping (один пакет за раз). Если ответа нет, сервер принимает адрес как неработающий и назначает его клиенту. При наличии ответа сервер принимает адрес как занятый и назначает другой адрес

Настройка тайм-аута Ping

Команда	**ip dhcp ping timeout** *milliseconds*
Описание параметров	*milli-seconds:* указывает время, необходимое серверу DHCP для ожидания ответа на эхо-запрос. Значение варьируется от 100 мс до 10000 мс
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	По умолчанию, если DHCP-сервер не получает ответ Ping в течение 500 мс, IP-адрес становится доступным. Вы можете настроить время ожидания для ответа сервера

4.4.7.6. Пример конфигурации

Настройка Ping

Этапы конфигурации	• Установите количество эхо-запросов на 5. • Установите тайм-аут ping на 800 мс
	QTECH(config)# ip dhcp ping packet 5 QTECH(config)# ip dhcp ping timeout 800
Проверка конфигурации	• Выполните команду **show run** для отображения конфигурации
	QTECH(config)#show run | begin ip dhcp ip dhcp ping packet 5 ip dhcp ping timeout 800

Настройка исключенного IP-адреса

Этапы конфигурации	• Настройте диапазон исключенных IP-адресов от 192.168.0.0 до 192.168.255.255
	QTECH(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
Проверка конфигурации	• Выполните команду **show run** для отображения конфигурации
	QTECH(config)#show run | begin ip dhcp ip dhcp excluded-address 192.168.0.0 192.168.255.255

4.4.8. Настройка основных функций DHCP Relay

4.4.8.1. Результат конфигурации

Развертывание динамического управления IP-сетями в режиме клиент-сервер для обеспечения связи между клиентом DHCP и сервером DHCP, которые находятся в разных сегментах сети.

4.4.8.2. Примечания

Для включения ретрансляции DHCP необходимо настроить одноадресную маршрутизацию IPv4 в сети.

4.4.8.3. Этапы конфигурации

Включение ретрансляции DHCP

- Обязательно.
- Если не указано иное, необходимо включить функцию DHCP Relay на устройстве.

Настройка IP-адреса для сервера DHCP

- Обязательно.
- Необходимо настроить IP-адрес для сервера DHCP.

4.4.8.4. Проверка конфигурации

Проверьте, получает ли клиент IP-адрес через DHCP Relay.

4.4.8.5. Связанные команды

Включение ретрансляции DHCP

Команда	**service dhcp**
Режим конфигурации	Режим глобальной конфигурации

Настройка IP-адреса для сервера DHCP

Команда	**ip helper-address { cycle-mode |** [**vrf** { *vrf-name* }] *A.B.C.D* **}**
Описание параметров	*cycle-mode*: указывает, что пакеты запросов DHCP пересылаются на все серверы DHCP. vrf-name: указывает имя маршрутизации и пересылки VPN (VRF). A.B.C.D: указывает IP-адрес сервера
Режим конфигурации	Режим глобальной конфигурации/режим конфигурации интерфейса

Встроенная подсказка	Эту функцию можно настроить на интерфейсе уровня 3, например, на маршрутизируемые порты, порты точки доступа уровня 3, SVI и интерфейс обратной связи. Настроенный интерфейс должен быть доступен через одноадресную маршрутизацию IPv4

4.4.8.6. Пример конфигурации

Настройка ретрансляции DHCP в проводном подключении

Сценарий:

Рисунок 4-15.

Этапы конфигурации	• Включите клиент с DHCP, чтобы получить IP-адрес. • Включите функцию DHCP Relay на агенте ретрансляции DHCP. • Настройка сервера DHCP
A	Включите клиент с DHCP, чтобы получить IP-адрес
B	Включите ретрансляцию DHCP. QTECH(config)# service dhcp Настройте глобальный IP-адрес сервера DHCP. QTECH(config)# ip helper-address 172.2.2.1 Настройте IP-адрес порта, подключенного к клиенту. QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if)# ip address 192.1.1.1 255.255.255.0 Настройте IP-адрес порта, подключенного к серверу. QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
C	Включите сервер DHCP. QTECH(config)# service dhcp Настройте пул адресов. QTECH(config)# ip dhcp pool relay QTECH (dhcp-config)#network 192.1.1.0 255.255.255.0 QTECH (dhcp-config)#default-router 192.1.1.1 Настройте IP-адрес порта, подключенного к Relay агенту.

	QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
Проверка конфигурации	Проверьте, получает ли клиент IP-адрес. • Проверьте, получает ли клиент IP-адрес. • Проверьте конфигурацию ретрансляции DHCP
A	Устройство пользователя получает IP-адрес
B	После входа в агент ретрансляции DHCP выполните команду **show running-config** в привилегированном режиме EXEC, чтобы отобразить конфигурацию DHCP Relay. QTECH# show running-config service dhcp ip helper-address 172.2.2.1 ! interface GigabitEthernet 0/1 ip address 192.1.1.1 255.255.255.0 ! interface GigabitEthernet 0/2 ip address 172.2.2.2 255.255.255.0 !

4.4.8.7. Типичные ошибки

- Неверная конфигурация одноадресной маршрутизации IPv4.
- Функция DHCP Relay отключена.
- Маршрутизация между агентом ретрансляции DHCP и сервером DHCP не настроена.
- Для сервера DHCP не настроен IP-адрес.

4.4.9. Настройка DHCP Relay опции 82

4.4.9.1. Результат конфигурации

С помощью агента ретрансляции DHCP сервер может более точно назначать IP-адреса с разными привилегиями клиентам на основе информации о параметре.

4.4.9.2. Примечания

Необходимо включить функцию ретрансляции DHCP.

4.4.9.3. Этапы конфигурации

Включение основных функций ретрансляции DHCP

- Обязательно.

- Если не указано иное, необходимо включить функцию DHCP Relay на устройстве.

Включение опции DHCP 82

- По умолчанию опция DHCP 82 отключена.
- Можно запустить команду **ip dhcp relay information option82**, чтобы включить или отключить DHCP Option 82.

4.4.9.4. Проверка конфигурации

Проверьте, получает ли клиент IP-адрес в соответствии с опцией 82.

4.4.9.5. Связанные команды

Включение опции DHCP 82

Команда	**ip dhcp relay information option82**
Режим конфигурации	Режим глобальной конфигурации

4.4.9.6. Пример конфигурации

Включение опции DHCP 82

Этапы конфигурации	• Включение опции DHCP 82
	QTECH(config)# ip dhcp relay information option82
Проверка конфигурации	После входа в агент ретрансляции DHCP выполните команду **show running-config** в привилегированном режиме EXEC, чтобы отобразить конфигурацию DHCP Relay
	QTECH#show ru | incl ip dhcp relay ip dhcp relay information option82

4.4.9.7. Типичные ошибки

Базовые функции ретрансляции DHCP не настроены.

4.4.10. Настройка проверки Server ID для DHCP Relay

4.4.10.1. Результат конфигурации

После настройки **ip dhcp relay check server-id** агент DHCP Relay пересылает пакеты запросов DHCP только серверу, указанному командой **option serverid**. В противном случае они пересылаются на все серверы DHCP.

4.4.10.2. Примечания

Необходимо включить базовые функции ретрансляции DHCP.

4.4.10.3. Этапы конфигурации

Включение DHCP Relay Check Server-ID

- По умолчанию идентификатор сервера проверки ретрансляции DHCP отключен.
- Можно запустить команду **ip dhcp relay check server-id**, чтобы включить DHCP Relay Check Server-id.

4.4.10.4. Проверка конфигурации

Убедитесь, что агент DHCP Relay отправляет пакеты запросов DHCP только на сервер, указанный командой **option server-id**.

4.4.10.5. Связанные команды

Настройка идентификатора сервера проверки ретрансляции DHCP

Команда	**ip dhcp relay check server-id**
Режим конфигурации	Режим глобальной конфигурации

4.4.10.6. Пример конфигурации

Настройка идентификатора сервера проверки ретрансляции DHCP

Этапы конфигурации	• Включение DHCP Relay. (Пропущено). • Включите **DHCP Relay check server-id** на интерфейсе
	QTECH# configure terminal QTECH(config)# ip dhcp relay check server-id
Проверка конфигурации	После входа в агент ретрансляции DHCP выполните команду **show running-config** в привилегированном режиме EXEC, чтобы отобразить конфигурацию DHCP Relay
	QTECH# show running-config | include check server-id ip dhcp relay check server-id

4.4.10.7. Типичные ошибки

Базовые функции ретрансляции DHCP не настроены.

4.4.11. Настройка подавления DHCP Relay

4.4.11.1. Результат конфигурации

После настройки команды **ip dhcp relay suppression** на интерфейсе пакеты DHCP Request, полученные на этом интерфейсе, будут отфильтрованы, а пакеты DHCP Request с других интерфейсов будут пересылаться.

4.4.11.2. Примечания

Необходимо включить базовые функции ретрансляции DHCP.

4.4.11.3. Этапы конфигурации

Включение подавления ретрансляции DHCP

По умолчанию функция подавления ретрансляции DHCP отключена на всех интерфейсах.

- Можно выполнить команду **ip dhcp relay suppression**, чтобы включить функцию DHCP Relay Suppression.

4.4.11.4. Проверка конфигурации

Проверьте, отфильтрованы ли пакеты запросов DHCP, полученные на интерфейсе.

4.4.11.5. Связанные команды

Настройка подавления DHCP-ретрансляции

Команда	**ip dhcp relay suppression**
Режим конфигурации	Режим конфигурации интерфейса

4.4.11.6. Пример конфигурации

Настройка подавления DHCP-ретрансляции

Этапы конфигурации	• Настройка основных функций ретрансляции DHCP. • Настройка подавления ретрансляции DHCP на интерфейсе
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ip dhcp relay suppression QTECH(config-if-GigabitEthernet 0/1)#end QTECH#
Проверка конфигурации	После входа в агент ретрансляции DHCP выполните команду **show running-config** в привилегированном режиме EXEC, чтобы отобразить конфигурацию DHCP Relay
	QTECH# show running-config | include relay suppression ip dhcp relay suppression QTECH#

4.4.11.7. Типичные ошибки

Базовые функции ретрансляции DHCP не настроены.

4.4.12. Настройка клиента DHCP

4.4.12.1. Результат конфигурации

Включите DHCP-клиент на устройстве, чтобы он динамически получил IP-адреса и конфигурации.

4.4.12.2. Примечания

Оборудование QTECH поддерживает конфигурацию клиента DHCP на интерфейсах Ethernet, FR, PPP и HDLC.

4.4.12.3. Этапы конфигурации

Запустите команду **ip address dhcp** на интерфейсе.

4.4.12.4. Проверка конфигурации

Проверьте, получает ли интерфейс IP-адрес.

4.4.12.5. Связанные команды

Настройка клиента DHCP

Команда	**ip address dhcp**
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	• Оборудование QTECH поддерживает динамическое получение IP-адресов через интерфейс Ethernet. • Оборудование QTECH поддерживает динамическое получение IP-адресов через инкапсулированный PPP-интерфейс. • Оборудование QTECH поддерживает динамическое получение IP-адресов посредством интерфейса, инкапсулированного FR. • Оборудование QTECH поддерживает динамическое получение IP-адресов посредством интерфейса, инкапсулированного HDLC

4.4.12.6. Пример конфигурации

Настройка клиента DHCP

Этапы конфигурации	• 1: Включите порт FastEthernet 0/0 с DHCP, чтобы получить IP-адрес
	QTECH(config)# interface FastEthernet0/0 QTECH(config-if-FastEthernet 0/0)#ip address dhcp

Проверка конфигурации	• 1: Выполните команду **show run** для отображения конфигурации
	QTECH(config)#show run | begin ip address dhcp ip address dhcp

4.5. Контроль состояния

4.5.1. Очистка

ВНИМАНИЕ: ВЫПОЛНЕНИЕ КОМАНД ОЧИСТКИ МОЖЕТ ПРИВЕСТИ К ПОТЕРЕ ВАЖНОЙ ИНФОРМАЦИИ И ПРЕРЫВАНИЮ СЛУЖБ.

Описание	Команда
Удаление привязки адреса DHCP	**clear ip dhcp binding** { *address* | *}
Очищает конфликт адресов DHCP	**clear ip dhcp conflict** { *address* | *}
Удаляет статистику сервера DHCP	**clear ip dhcp server statistics**
Удаляет статистику ретрансляции DHCP	**clear ip dhcp relay statistics**
Очистка статистики производительности DHCP-сервера	**clear ip dhcp server rate**

4.5.2. Отображение

Описание	Команда
Отображение аренды DHCP	**show dhcp lease**
Отображение IP-адресов, настроенных вручную	**show dhcp manual**
Отображение сокетов DHCP	**show ip dhcp socket**
Отображение назначенных IP-адресов	**show ip dhcp binding**

Описание	Команда
Отображение статистики сервера DHCP	**show ip dhcp server statistic**
Отображение статистики ретрансляции DHCP	**show ip dhcp relay statistic**
Отображение конфликтующих адресов	**show ip dhcp conflict**

4.5.3. Отладка

ПРИМЕЧАНИЕ: системные ресурсы используются при выводе отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Отладка агента DHCP	**debug ip dhcp server agent**
Отладка горячего резервного копирования DHCP	**debug ip dhcp server ha**
Отладка пулов адресов DHCP	**debug ip dhcp server pool**
Отладка DHCP VRRP	**debug ip dhcp server vrrp**
Отладка всех серверов DHCP	**debug ip dhcp server all**
Отладка пакетов DHCP	**debug ip dhcp client**
Отладка событий ретрансляции DHCP	**debug ip dhcp relay**

5. НАСТРОЙКА DHCPV6

5.1. Обзор

Протокол динамической конфигурации хоста для IPv6 (DHCPv6) — это протокол, который позволяет серверу DHCP передавать конфигурации (например, адреса IPv6) узлам IPv6.

По сравнению с другими методами распределения адресов IPv6, такими как ручная настройка и автоматическая настройка адресов без сохранения состояния, DHCPv6 обеспечивает распределение адресов, делегирование префиксов и распределение параметров конфигурации.

- DHCPv6 — это протокол с отслеживанием состояния для автоматической настройки адресов, а также добавления, и повторного использования сетевых адресов, который позволяет записывать выделенные адреса и оптимизировать управление сетью.
- Используя префикс делегирования DHCPv6, сетевые устройства uplink могут назначать префиксы адресов сетевым устройствам downlink, которые реализуя гибкую автоматическую конфигурацию на уровне станции и гибкое управление адресным пространством станции.
- Назначение параметра конфигурации DHCPv6 решает проблему, при которой параметры не могут быть получены с помощью протокола автоматической настройки адресов без сохранения состояния, и назначает адреса DNS-серверов и имена доменов хостам.
- DHCPv6 — это протокол, основанный на модели клиент-сервер. Клиент DHCPv6 используется для получения различных конфигураций, а сервер DHCPv6 используется для предоставления различных конфигураций. Если клиент DHCPv6 и сервер DHCPv6 не подключены к одному сетевому каналу (один и тот же сегмент сети), они могут взаимодействовать друг с другом с помощью агента ретрансляции DHCPv6.

Клиент DHCPv6 обычно обнаруживает сервер DHCPv6, резервируя адреса многоадресной рассылки в канале, поэтому клиент DHCPv6 и сервер DHCPv6 должны иметь возможность напрямую взаимодействовать друг с другом, то есть они должны быть развернуты в пределах одного канала. Это может привести к неудобствам в управлении, экономическим сбоям (для каждой подсети развернут сервер DHCPv6) и неудобствам при обновлении. Функция агента ретрансляции DHCPv6 может решить эти проблемы, позволяя клиенту DHCPv6 отправлять пакеты на сервер DHCPv6 по другому каналу. Агент ретрансляции DHCP часто развертывается в канале, где находится клиент DHCPv6, и используется для ретрансляции пакетов взаимодействия между клиентом DHCPv6 и сервером DHCPv6. Агент ретрансляции DHCP прозрачен для клиента DHCPv6.

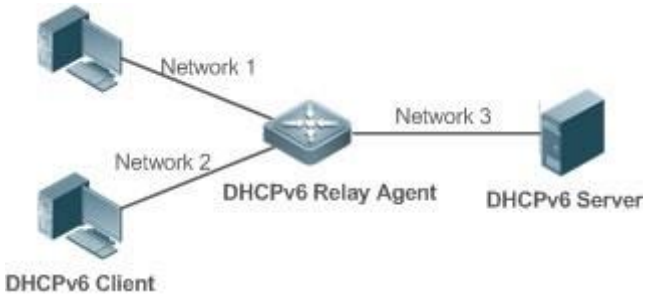


Рисунок 5-1.

5.1.1. Протоколы и стандарты

- RFC3315: протокол динамической конфигурации хоста для IPv6.
- RFC3633: параметры префикса IPv6 для протокола динамической конфигурации хоста (DHCP) версии 6.
- RFC3646: параметры конфигурации DNS для протокола динамической конфигурации хоста для IPv6 (DHCPv6).
- RFC3736: служба DHCP без сохранения состояния для IPv6.
- RFC5417: управление и настройка опции DHCP контроллера доступа к беспроводным точкам доступа (CAPWAP).

5.2. Применение

Применение	Описание
Запрос/назначение адресов и параметров конфигурации	Клиент DHCPv6 запрашивает адреса с сервера DHCPv6. Сервер DHCPv6 назначает адреса и параметры конфигурации клиенту DHCPv6
Запрос/выделение префикса	Клиент DHCPv6 запрашивает префикс с сервера DHCPv6. Сервер DHCPv6 присваивает префикс клиенту DHCPv6, а затем клиент DHCPv6 настраивает адреса IPv6 с помощью этого префикса
Ошибка! Источник ссылки не найден.	DHCPv6 Relay используется для обеспечения связи между клиентом DHCPv6 и сервером DHCPv6 по разным каналам

5.2.1. Запрос/назначение адресов и параметров конфигурации

5.2.1.1. Сценарий

В подсети клиент DHCPv6 запрашивает адреса с сервера DHCPv6. Сервер DHCPv6 назначает адреса и параметры конфигурации клиенту DHCPv6.

Как показано на Рисунке 5-2:

- Сервер DHCPv6 настроен с адресами IPv6, DNS-серверами, доменными именами и другими параметрами конфигурации, которые необходимо выделить.
- Хост работает как клиент DHCPv6 для запроса адреса IPv6 с сервера DHCPv6. После получения запроса сервер DHCPv6 выбирает доступный адрес и назначает его хосту.
- Хост также может запросить DNS-сервер, имя домена и другие параметры конфигурации с сервера DHCPv6.

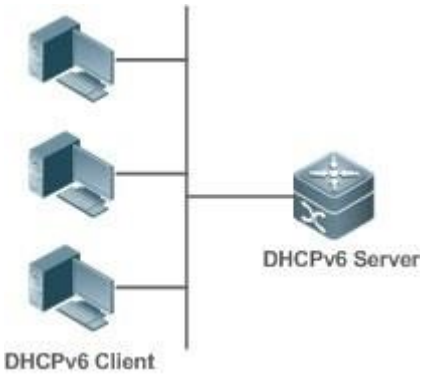


Рисунок 5-2.

5.2.1.2. Описание

- Запустите клиент DHCPv6 на хосте в подсети, чтобы получить адрес IPv6 и другие параметры.
- Запустите сервер DHCPv6 на устройстве и настройте IPv6-адрес и другие параметры, чтобы назначить IPv6-адрес и параметры.

5.2.2. Запрос/выделение префикса

5.2.2.1. Сценарий

Как показано на Рисунке 5-3, uplink-устройство (PE) выделяет префикс IPv6-адреса для устройства downlink (CPE). CPE генерирует новый префикс адреса для внутренней подсети на основе полученного префикса. Хосты во внутренней подсети CPE конфигурируются с адресами через Router Advertisement (RA), используя новый префикс адреса.

- PE предоставляет службу делегирования префикса в качестве сервера DHCPv6.
- CPE запрашивает префикс адреса из PE в качестве клиента DHCPv6. После получения префикса адреса CPE генерирует новый префикс адреса для внутренней подсети и отправляет сообщение RA хостам во внутренней подсети.
- Хосты во внутренней подсети, в которой находится CPE, настраивают свои адреса на основании сообщения RA, отправленного CPE.

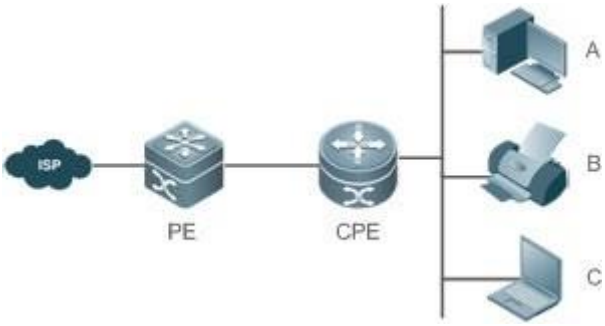


Рисунок 5-3.

В качестве сервера DHCPv6 Provider Edge (PE) работает сервер поставщика для предоставления префиксов, а также называется маршрутизатором для делегирования.

Клиентское оборудование (CPE) работает как клиент DHCPv6 для запроса префиксов и также называется запрашивающим маршрутизатором.

A, B и C являются различными хостами.

5.2.2.2. Описание

- Запустите сервер DHCPv6 на PE, чтобы внедрить службу делегирования префикса.
- Запустите клиент DHCPv6 на CPE, чтобы получить префиксы адресов.
- Разверните IPv6 ND между CPE и хостами, чтобы настроить адреса узлов в подсети через RA.

5.2.3. Агент Relay

5.2.3.1. Сценарий

Агент DHCPv6 Relay производит ретрансляцию DHCPv6 пакетов между клиентом и сервером.

Как показано на Рисунке 5-4:

- Устройство 1 включено с помощью агента DHCPv6 Relay и предназначено для 3001:2.
- Устройство 2 хочет пересылать пакеты на другие серверы через сервис Relay следующего уровня. Включите агент DHCPv6 Relay на устройстве 2, установите адрес назначения FF02::1:2 (все серверы и адреса многоадресной рассылки Relay) и укажите интерфейс выхода в качестве интерфейса уровня 3 gi 0/1.

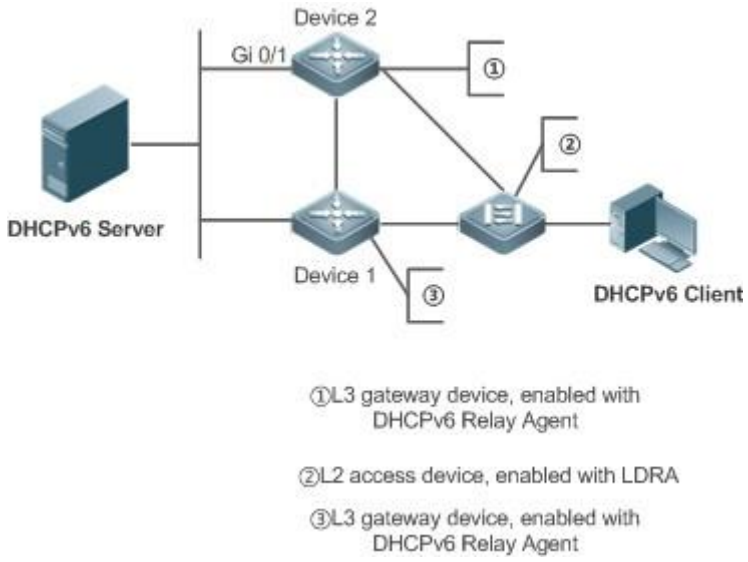


Рисунок 5-4.

5.2.3.2. Описание

- Включите агент DHCPv6 Relay на устройстве 1 и укажите адрес 3000::1.
- Включите агент DHCPv6 Relay на устройстве 2 и укажите адрес как FF02::1:2.

5.3. Ключевые особенности

5.3.1. Базовые концепции

DUID

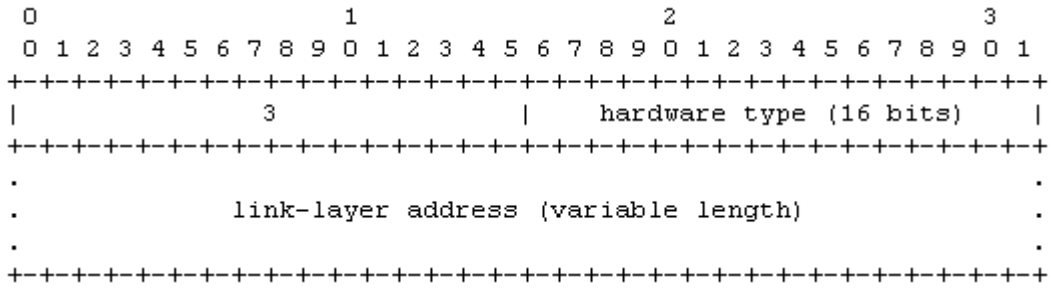
Уникальный идентификатор DHCP (DUID) идентифицирует устройство DHCPv6. Как определено в RFC3315, каждое устройство DHCPv6 (клиент, Relay или сервер DHCPv6)

должно иметь идентификатор DUID, который используется для взаимной аутентификации во время обмена сообщениями DHCPv6.

RFC3315 определяет три типа DUID:

- DUID основан на адресе уровня связи плюс время (DUID-LLT).
- Идентификатор DUID, назначенный поставщиком на основе корпоративного номера (DUID-EN).
- Адрес уровня канала (DUID-LL).

Устройства QTECH DHCPv6 используют DUID-LL. Структура DUID-LL следующая:



Значения *DUID-LL*, *Hardware type* и *Link-layer address*: 0x0003, 0x0001 (с указанием Ethernet) и MAC-адреса устройства соответственно.

Ассоциация идентификации (IA)

Сервер DHCPv6 выделяет службы проверки подлинности в Интернете клиентам DHCPv6. Каждая IA уникально обнаруживается идентификатором ассоциации хостов (IAID). Идентификаторы IAID генерируются клиентами DHCPv6. Между IA и клиентами устанавливается сопоставление «один к одному». IA может содержать несколько адресов, которые могут быть выделены клиентом другим интерфейсам. IA может содержать один из следующих типов адресов:

- Невременные адреса (NA), а именно глобальные уникальные адреса.
- Временные адреса (TA), которые вряд ли используются.
- Делегирование префикса (PD).

В зависимости от типа адреса, IA классифицируются по IA_NA, IA_TA и IA_PD (три типа IA). QTECH DHCPv6 поддерживают только IA_NA и IA_PD.

Привязка

DHCPv6 binding — это управляемая информационная структура адреса. Данные привязки адресов на сервере DHCPv6 записывают IA и другие конфигурации каждого клиента. Клиент может запросить несколько привязок. Данные привязки адресов на сервере представлены в виде таблицы привязки адресов с идентификаторами DUID, IA-Type и IAID. Привязка, содержащая конфигурации, использует в качестве индекса DUID.

Конфликт DHCPv6

Когда происходит конфликт адреса, выделенного клиенту DHCPv6, клиент отправляет пакет Decline, чтобы уведомить сервер DHCPv6. Затем сервер добавляет адрес в список конфликтов адресов. Сервер не будет назначать адреса в список конфликтов адресов. Сервер поддерживает просмотр и удаление информации об адресе в списке конфликтов адресов.

Тип пакета

RFC3315 предусматривает, что DHCPv6 использует порты UDP 546 и 547 для обмена пакетами. В частности, клиент DHCPv6 использует порт 546 для получения пакетов, а сервер DHCPv6 и агент DHCPv6 Relay используют порт 547 для получения пакетов.

RFC3315 определяет следующие типы пакетов, которые передаются между сервером, клиентом и агентом DHCPv6 Relay:

- Пакеты, которые могут быть отправлены клиентом DHCPv6 на сервер DHCPv6, включают в себя Solicit, Request, Confirm, Renew, Rebind, Release, Decline и Information-request.
- Пакеты, которые могут быть отправлены сервером DHCPv6 клиенту DHCPv6, включают в себя Advertise, Reply and Reconfigure.
- Пакеты, которые могут быть отправлены агентом DHCPv6 Relay другому агенту DHCPv6 Relay или серверу DHCPv6, включают Relay-forward.
- Пакеты, которые могут быть отправлены агентом DHCPv6 Relay другому агенту DHCPv6 Relay или серверу DHCPv6, включают Relay-reply.

ПРИМЕЧАНИЕ: серверы QTECH DHCPv6 не поддерживают пакет Reconfigure.

ПРИМЕЧАНИЕ: клиенты QTECH DHCPv6 не поддерживают пакеты Confirm and Reconfigure.

5.3.2. Обзор

Функция	Описание
Запрос/выделение адресов	Динамическое получение/выделение адресов IPv6 в сети в режиме клиент-сервер
Запрос/выделение префикса	Динамическое получение/выделение префиксов IPv6 в сети в режиме клиент-сервер
Служба без сохранения состояния	Предоставляет службу конфигурации без сохранения состояния для хостов в сети
Сервис Relay	Предоставляет службу сервера DHCPv6 для хостов в различных сетях с помощью службы ретрансляции

5.3.3. Запрос/выделение адресов

Клиент DHCPv6 может запрашивать адреса IPv6 с сервера DHCPv6.

После настройки с доступными адресами сервер DHCPv6 может предоставлять адреса IPv6 хостам в сети, записывать выделенные адреса и улучшать управление сетью.

5.3.3.1. Принцип работы

Сетевые хосты служат клиентами DHCPv6 и серверами DHCPv6 для реализации распределения адресов, обновления, подтверждения, выпуска и других операций посредством обмена сообщениями.

Обмен 4-х сообщений

На Рисунке 5-5 показан процесс обмена четырех сообщений.

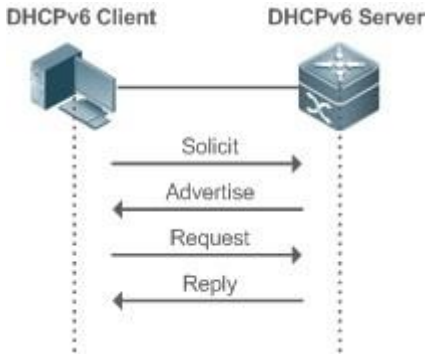


Рисунок 5-5.

- Клиент DHCPv6 отправляет сообщение Solicit, адрес назначения которого FF02::1:2, а номер порта назначения — 547 в локальной сети для запроса адреса, префикса и назначения параметров конфигурации. Все серверы DHCPv6 или агенты DHCPv6 Relay в широковещательном домене получат сообщение запроса.
- После получения сообщения запроса сервер DHCPv6 отправит сообщение Advertise в режиме одноадресной рассылки, если он сможет предоставить информацию, запрошенную в сообщении запроса. В сообщении объявления указаны адрес, префикс и параметры конфигурации.
- Клиент DHCPv6 может получать сообщение Advertise с нескольких серверов DHCPv6. После выбора наиболее подходящего сервера DHCPv6 клиент DHCPv6 отправляет сообщение Request с адресом назначения FF02::1:2, а номер порта назначения — 547 для запроса адреса, префикса и назначения параметров конфигурации.
- После получения сообщения Request сервер DHCPv6 создает привязку локально и отправляет сообщение Reply в режиме одноадресной рассылки. В сообщении для ответа содержатся адрес, префикс и параметры конфигурации, которые сервер DHCPv6 будет назначать клиенту DHCPv6. Клиент DHCPv6 получает адрес, префикс или параметры конфигурации на основе информации в сообщении ответа.

Обмен двумя сообщениями

Обмен двумя сообщениями может использоваться для более быстрого завершения настройки адресов, префиксов и параметров для клиентов DHCPv6.

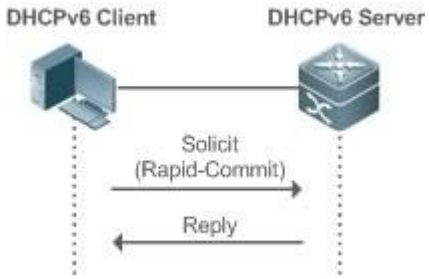


Рисунок 5-6.

- Клиент DHCPv6 отправляет сообщение запроса, адрес назначения которого FF02::1:2, а номер порта назначения — 547 в локальной сети для запроса адреса, префикса и назначения параметров конфигурации. Сообщение о ходатайстве содержит быструю фиксацию.
- Если сервер DHCPv6 поддерживает функцию быстрой фиксации (rapid commit), сервер DHCPv6 создает привязку локально и отправляет сообщение ответа в

режиме одноадресной рассылки. В сообщении для ответа содержатся адрес, префикс и параметры конфигурации, которые будут назначены клиенту DHCPv6. Клиент DHCPv6 завершает настройку на основе информации в сообщении ответа.

Обновление и перепривязка

Сервер DHCPv6 предоставляет управляющий адрес и обновленные T1 и T2 в IA сообщения, отправленного клиенту DHCPv6.

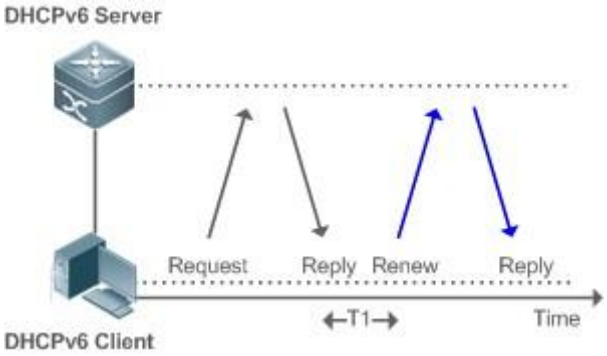


Рисунок 5-7.

- Клиент DHCPv6 отправит многоадресное сообщение Renew на сервер DHCPv6 для обновления адреса и префикса через T1 секунд. Сообщение Renew содержит идентификатор DUID сервера DHCPv6 и информацию IA, которую необходимо обновить.
- После получения сообщения о возобновлении сервер DHCPv6 проверяет, равно ли значение DUID в сообщении о возобновлении значению DUID локального устройства. Если да, то сервер DHCPv6 обновляет локальную привязку и отправляет сообщение для ответа в режиме одноадресной рассылки. В сообщении для ответа содержатся новые T1 и другие параметры.

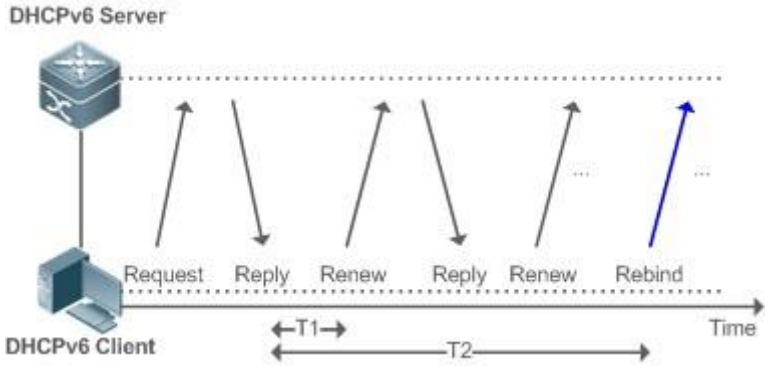


Рисунок 5-8.

- Если после отправки клиентом DHCPv6 сообщения о возобновлении на сервер DHCPv6 ответ не получен, клиент DHCPv6 отправит на сервер DHCPv6 многоадресное сообщение о повторной привязке для перепривязки адреса и префикса после истечения срока действия T2.
- После получения сообщения Rebind сервер DHCPv6 (возможно, новый сервер DHCPv6) отправляет сообщение с ответом в соответствии с содержимым сообщения Rebind.

Release

Если клиенту DHCPv6 требуется освободить адрес или префикс, клиенту DHCPv6 необходимо отправить сообщение Release на сервер DHCPv6, чтобы уведомить сервер

DHCPv6 об освобождении адреса или префикса. Таким образом, сервер DHCPv6 может назначить эти адреса и префиксы другим клиентам DHCPv6.

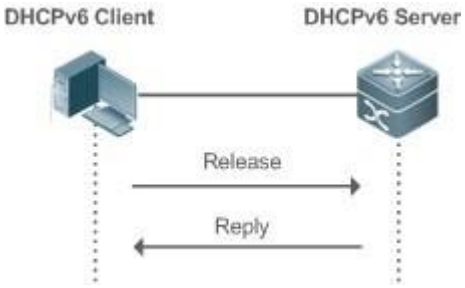


Рисунок 5-9.

- После получения сообщения Release сервер DHCPv6 удаляет соответствующие привязки на основе адресов или префиксов в сообщении релиза и отправляет ответное сообщение с параметром состояния клиенту DHCPv6.

Подтверждение (Confirmation)

После перехода к новой ссылке (например, после перезапуска) клиент DHCPv6 отправит сообщение Confirm на сервер DHCPv6 по новой ссылке, чтобы проверить, доступны ли исходные адреса.

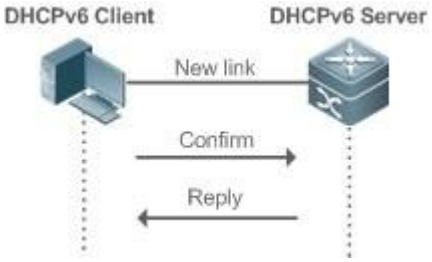


Рисунок 5-10.

- После получения сообщения о подтверждении сервер DHCPv6 выполняет подтверждение на основе информации об адресе в сообщении о подтверждении и отправляет сообщение с запросом, в котором имеется опция состояния, клиенту DHCPv6. Если запрос не будет подтвержден, клиент DHCPv6 может инициировать новый запрос на выделение адресов.

Конфликт DHCPv6

Если клиент DHCPv6 обнаруживает, что выделенные адреса были использованы в канале после завершения выделения адресов, клиент DHCPv6 отправляет сообщение Decline, чтобы уведомить сервер DHCPv6 о конфликте адресов.

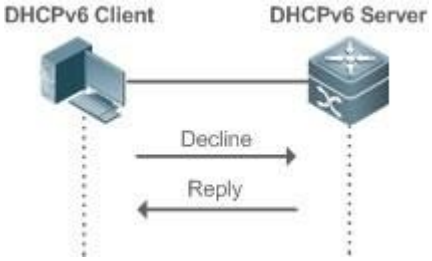


Рисунок 5-11.

Клиент DHCPv6 содержит информацию IA о конфликтующих адресах в сообщении Decline.

- После получения сообщения Decline сервер DHCPv6 помечает адреса в сообщении Decline как "отклоненные" и не будет распределять эти адреса. Затем

сервер DHCPv6 отправляет сообщение Reply с параметром состояния клиенту DHCPv6. Можно вручную удалить адреса, помеченные как «отклоненные», чтобы облегчить повторное выделение.

5.3.3.2. Связанная конфигурация

Включение функции сервера DHCPv6 в интерфейсе

- По умолчанию интерфейс не включен с функцией сервера DHCPv6.
- Можно выполнить команду **ipv6 dhcp server**, чтобы включить функцию DHCPv6 Server для интерфейса.

ПРИМЕЧАНИЕ: функция сервера DHCPv6 должна быть включена на интерфейсе уровня 3.

Выделение адресов через сервер DHCPv6

- По умолчанию на сервере DHCPv6 отсутствует пул конфигурации и не настроены адреса для выделения.
- Для создания пула конфигурации можно выполнить команду **ipv6 dhcp pool**.
- Можно выполнить команду **iana-address**, чтобы настроить адреса для выделения, а также предпочтительные значения срока службы **preferred lifetime** и текущего срока службы **valid lifetime**.

Удаление конфликтующих адресов через сервер DHCPv6

- По умолчанию сервер DHCPv6 не выполняет очистки обнаруженных конфликтующих адресов.
- Можно выполнить команду **clear ipv6 dhcp conflict** для очистки конфликтующих адресов, чтобы эти адреса можно было использовать повторно.

5.3.4. Запрос/выделение префикса

Настройка доступных префиксов на сервере DHCPv6. Используя префикс делегирования DHCPv6, сетевые устройства uplink могут назначать префиксы адресов сетевым устройствам downlink, которые реализуя гибкую автоматическую конфигурацию на уровне станции и гибкое управление адресным пространством станции.

5.3.4.1. Принцип работы

Сетевые устройства нисходящего канала служат клиентами DHCPv6 для обмена сообщениями с сервером DHCPv6 для реализации операций allocation, update, release и других операций. Сетевые устройства downlink получают, обновляют, связывают и освобождают префиксы с помощью механизма обмена сообщениями, аналогичного механизму распределения адресов. Однако назначение префиксов отличается от назначения адресов в следующих аспектах:

При обмене сообщениями с использованием делегирования префикса, сообщения подтверждения и отклонения не используются.

Если клиент DHCPv6 переходит на новую ссылку и ему необходимо проверить, доступна ли информация префикса, он выполняет подтверждение посредством обмена сообщениями Rebind и Reply.

Тип IA в различных сообщениях — IA_PD.

ПРИМЕЧАНИЕ: для обмена сообщениями с использованием делегирования префикса см. раздел Запрос/выделение адресов.

5.3.4.2. Связанная конфигурация

Включение функции сервера DHCPv6 в интерфейсе

- По умолчанию функционал DHCPv6 сервера не включен на интерфейсе.
- Можно выполнить команду **ipv6 dhcp server**, чтобы включить функцию DHCPv6 Server для интерфейса.

ПРИМЕЧАНИЕ: функция сервера DHCPv6 действует только на интерфейсе уровня 3.

Делегирование префиксов сервера DHCPv6

- По умолчанию на сервере DHCPv6 нет конфигурации пула и префиксов.
- Для конфигурации пула можно выполнить команду **ipv6 dhcp pool**.
- Можно выполнить команду **prefix-delegation**, чтобы назначить указанные префиксы конкретному клиенту DHCPv6.
- Можно запустить команду **prefix-delegation pool**, чтобы настроить пул префиксов таким образом, чтобы все префиксы, запрошенные клиентом DHCPv6, были выделены из этого пула.

5.3.5. Служба без сохранения состояния

Если клиенту DHCPv6 требуются только параметры конфигурации, служба DHCPv6 без сохранения состояния может использоваться для получения связанных параметров конфигурации, которые невозможно получить с помощью протокола автоматической настройки адресов без сохранения состояния, например, адреса DNS-сервера.

5.3.5.1. Принцип работы

Сетевые хосты служат клиентами DHCPv6 для обмена сообщениями с сервером DHCPv6 для получения и обновления параметров конфигурации.

Обмен сообщениями с помощью службы без сохранения состояния

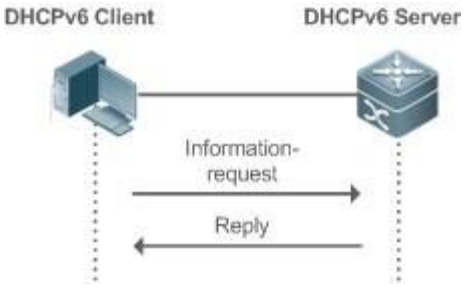


Рисунок 5-12.

Клиент DHCPv6 отправляет сообщение запроса информации на сервер DHCPv6 для запроса сообщений без сохранения состояния. Обычно это сообщение не содержит идентификатор DUID указанного сервера DHCPv6.

Сервер DHCPv6 отправляет клиенту DHCPv6 сообщение с параметрами конфигурации.

5.3.5.2. Связанная конфигурация

Включение функции сервера DHCPv6 в интерфейсе

- По умолчанию интерфейс не включен с функцией сервера DHCPv6.
- Можно запустить команду **ipv6 dhcp server**, чтобы включить или отключить функцию DHCPv6 Server для интерфейса.

ПРИМЕЧАНИЕ: функция сервера DHCPv6 действует только на интерфейсе уровня 3.

Служба без сохранения состояния сервера DHCPv6

- По умолчанию на сервере DHCPv6 отсутствует пул конфигурации и не настроены параметры конфигурации.
- Для создания пула конфигурации можно выполнить команду **ipv6 dhcp pool**.
- Для добавления DNS-сервера можно выполнить команду **dns-server**.
- Чтобы добавить имя домена, можно выполнить команду **domain-name**.
- Можно запустить команду **option52**, чтобы добавить IPv6-адрес AC CAPWAP.

5.3.6. DHCPv6 Relay

Когда клиент DHCPv6 и сервер DHCPv6 находятся по разным каналам, клиент DHCPv6 может передавать связанные сообщения на сервер DHCPv6 через агента ретрансляции DHCPv6. Сервер DHCPv6 также передает ответ клиенту DHCPv6 через агента ретрансляции.

5.3.6.1. Принцип работы

При получении сообщения от клиента DHCPv6 агент ретрансляции DHCPv6 создает сообщение Relay-forward. Это сообщение содержит исходное сообщение от клиента DHCPv6 и некоторые параметры, добавленные агентом ретрансляции.

Затем агент ретрансляции отправляет сообщение Relay-forward на указанный сервер DHCPv6 или указанный адрес многоадресной рассылки FF05::1:3.

После получения сообщения Relay-forward сервер DHCPv6 извлекает исходное сообщение из клиента DHCPv6 для обработки. Затем сервер DHCPv6 формирует ответ на исходное сообщение, инкапсулирует ответ в сообщении Relay-Reply и отправляет сообщение Relay-Reply агенту DHCPv6 Relay.

После получения сообщения Relay-Reply агент ретрансляции DHCPv6 извлекает исходное сообщение с сервера DHCPv6 для обработки и пересылает сообщение клиенту DHCPv6.

Между клиентом DHCPv6 и сервером DHCPv6 разрешены многоуровневые Relay агенты.

Агент ретрансляции DHCPv6

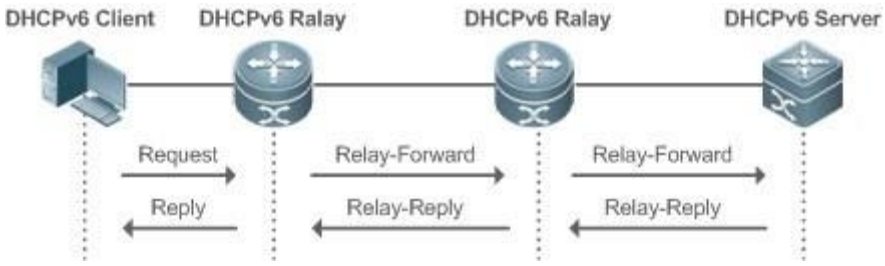


Рисунок 5-13.

Агент ретрансляции DHCPv6 выполняет инкапсуляцию и декапсуляцию сообщений между клиентом DHCPv6 и сервером DHCPv6 для обеспечения связи между клиентом DHCPv6 и сервером DHCPv6 по разным каналам.

5.4. Настройка

Настройка	Описание и команда	
Настройка сервера DHCPv6	(Обязательно) используется для создания пула конфигурации	
	ipv6 dhcp pool	Настройка пула конфигурации для сервера DHCPv6
	(Необязательно) используется для назначения адресов	
	iana-address prefix	Настройка префиксов адресов, которые будут выделены на сервере DHCPv6
	(Необязательно) используется для назначения префиксов	
	prefix-delegation	Настройка префиксов статически привязанных адресов на сервере DHCPv6
	prefix-delegation pool	Настройка сервера DHCPv6 для выделения префиксов из локального пула префиксов
	ipv6 local pool	Настройка локального пула префиксов IPv6
	(Необязательно) используется для назначения параметров конфигурации	
	dns-server	Настройка DNS-сервера на сервере DHCPv6
	domain-name	Настройка имени домена сервера DHCPv6
	option52	Настройка IPv6-адреса CAPWAP AC на сервере DHCPv6
	(Обязательно) используется для включения службы сервера DHCPv6	
	ipv6 dhcp server	Включение службы сервера DHCPv6 на интерфейсе

Настройка	Описание и команда	
Настройка DHCPv6 Relay	(Обязательно) используется для включения службы агента ретрансляции DHCPv6	
	ipv6 dhcp relay destination	Настройка функции агента ретрансляции DHCPv6

5.4.1. Настройка сервера DHCPv6

5.4.1.1. Результат конфигурации

Uplink-устройство может автоматически назначать адреса DHCPv6, префиксы и параметры конфигурации устройству нисходящего канала.

5.4.1.2. Примечания

- Для предоставления серверной службы DHCPv6 необходимо указать пул сервера DHCPv6.
- Имя пула не может быть слишком длинным.
- При включении службы сервера DHCPv6 необходимо указать пул.
- Эта конфигурация поддерживается только для виртуального интерфейса коммутатора (SVI), маршрутизируемого порта и агрегированного порта L3 (AP).

5.4.1.3. Этапы конфигурации

Настройка пула сервера DHCPv6

- Обязательно.
- Если не указано иное, необходимо настроить пул сервера DHCPv6 на всех устройствах, которые должны обеспечить службу сервера DHCPv6.

Настройка префиксов адресов, которые будут выделены на сервере DHCPv6

- Опционально.
- Для предоставления службы распределения адресов необходимо настроить префиксы адресов, которые будут выделены на всех устройствах, которые должны предоставить службу сервера DHCPv6.

Настройка префикса статических адресов на сервере DHCPv6

- Опционально.
- Чтобы предоставить службу делегирования префиксов для статически привязанных адресов, необходимо настроить префиксы статически привязанных адресов на всех устройствах, которые должны предоставить службу сервера DHCPv6.

Настройка сервера DHCPv6 для выделения префиксов из пула локальных префиксов

- Опционально.
- Для предоставления службы делегирования префиксов необходимо указать локальный пул префиксов на всех устройствах, которым требуется предоставить службу сервера DHCPv6.

Настройка пула префиксов Local IPv6

- Опционально.
- Для предоставления службы делегирования префиксов через пул префиксов необходимо указать локальный пул префиксов на всех устройствах, которые должны предоставить службу сервера DHCPv6.

Настройка DNS-сервера на сервере DHCPv6

- Опционально.
- Чтобы выделить DNS-серверы, необходимо настроить DNS-сервер на всех устройствах, которые должны предоставить службу сервера DHCPv6.

Настройка имен доменов на сервере DHCPv6

- Опционально.
- Чтобы назначить доменные имена, необходимо настроить имена доменов на всех устройствах, которые должны предоставить службу сервера DHCPv6.

Настройка IPv6-адреса CAPWAP AC на сервере DHCPv6

- Опционально.
- Чтобы выделить информацию CAPWAP AC, необходимо настроить IPv6-адрес CAPWAP AC на всех устройствах, которые должны предоставить службу сервера DHCPv6.

Включение службы сервера DHCPv6

- Обязательно.
- Если не указано иное, необходимо включить службу сервера DHCPv6 на определенных интерфейсах всех устройств, которые должны обеспечить службу сервера DHCPv6.

5.4.1.4. Проверка конфигурации

Сервер DHCPv6 выделяет адреса, префиксы или параметры конфигурации для клиента DHCPv6.

- Клиент DHCPv6 получает необходимую информацию.
- Сервер DHCPv6 успешно создает локальную привязку.

5.4.1.5. Связанные команды

Настройка пула конфигурации сервера DHCPv6

Команда	**ipv6 dhcp pool** *poolname*
Описание параметров	***poolname***: указывает имя определяемого пользователем пула DHCPv6
Режим конфигурации	Режим глобальной конфигурации

Встроенная подсказка	Выполните команду **ipv6 dhcp pool**, чтобы создать пул сервера DHCPv6. После настройки этой команды можно войти в режим конфигурации пула DHCPv6, в котором можно настроить такие параметры пула, как префикс и DNS-сервер. После создания пула конфигурации сервера DHCPv6 можно выполнить команду **ipv6 dhcp server**, чтобы связать пул со службой сервера DHCPv6 на интерфейсе

Настройка префикса адреса IA_NA для сервера DHCPv6

Команда	**iana-address prefix** *ipv6-prefix/prefix-length* [**lifetime** { *validlifetime* | *preferred-lifetime* }]
Описание параметров	*ipv6-prefix/prefix-length*: указывает префикс адреса IPv6 и длину префикса. lifetime: устанавливает допустимое время адреса, назначенного клиенту. Это ключевое слово должно быть настроено вместе с *valid-lifetime* (действительным сроком службы) и *preferred-lifetime* (предпочтительным сроком службы). *valid-lifetime*: указывает допустимое время адреса, назначенного клиенту. *preferred-lifetime*: указывает время, когда адрес назначается клиенту в первую очередь
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Выполните команду **iana-address prefix**, чтобы настроить префиксы адресов IA_NA для сервера DHCPv6, некоторые из которых выделены клиенту. При получении запроса на адрес IA_NA от клиента сервер DHCPv6 выбирает доступный адрес в соответствии с диапазоном адресов IA_NA и назначает адрес клиенту. Если клиент не использует этот адрес, сервер DHCPv6 помечает этот адрес как доступный для другого клиента

Настройка префикса статически привязанных адресов на сервере DHCPv6

Команда	**prefix-delegation** *ipv6-prefix/prefix-length client-DUID* [*lifetime*]
Описание параметров	*ipv6-prefix/prefix-length*: указывает префикс адреса IPv6 и длину префикса. *client-DUID*: указывает идентификатор DUID клиента. *lifetime*: устанавливает время, в течение которого клиент может использовать этот префикс

Режим конфигурации	Режим конфигурации пула DHCPv6
Встроенная подсказка	Вы можете запустить команду **prefix-delegation**, чтобы вручную настроить список префиксов для IA_PD клиента и указать допустимое время для этих префиксов. Используйте параметр *client-DUID* для указания клиента, которому назначен префикс адреса. Префикс адреса будет назначен первому IA_PD клиента. После получения запроса на префикс адреса от клиента сервер DHCPv6 проверяет, доступна ли статическая привязка. Если да, то сервер DHCPv6 напрямую возвращает статическую привязку. В противном случае сервер DHCPv6 выделяет префикс адреса из другого источника префикса

Настройка сервера DCHPv6 для выделения префиксов из пула локальных префиксов

Команда	**prefix-delegation pool** *poolname* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]
Описание параметров	***poolname*:** указывает имя определенного пользователем пула локальных префиксов. **lifetime:** устанавливает допустимое время префикса, назначенного клиенту. Это ключевое слово должно быть настроено вместе с *valid-lifetime* (действительным сроком службы) и *preferred-lifetime* (предпочтительным сроком службы). *valid-lifetime*: указывает допустимое время префикса, назначенного клиенту. *preferred-lifetime*: указывает время, в течение которого префикс преимущественно назначается клиенту
Режим конфигурации	Режим конфигурации пула DHCPv6
Встроенная подсказка	Выполните команду пула делегирования префиксов, чтобы настроить пул префиксов для сервера DHCPv6 для выделения префиксов клиентам. Команда **ipv6 local pool** используется для настройки пула префиксов. При получении запроса на префикс от клиента сервер DHCPv6 выбирает доступный префикс из пула префиксов и назначает префикс клиенту. Если клиент не использует этот префикс, сервер DHCPv6 получает префикс

Настройка пула префиксов Local IPv6

Команда	**ipv6 local pool** *poolname prefix/prefix-length assigned-length*
Описание параметров	*poolname*: указывает имя локального пула префиксов. *prefix/prefix-length***:** указывает префикс и длину префикса. *assigned-length***:** указывает длину префикса, назначенного пользователю
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Выполните команду **ipv6 local pool**, чтобы создать локальный пул префиксов. Если серверу DHCPv6 требуется делегирование префиксов, можно запустить команду **prefix-delegation pool**, чтобы указать локальный пул префиксов. После этого префиксы будут выделены из указанного локального пула префиксов

Настройка DNS-сервера на сервере DHCPv6

Команда	**dns-server** *ipv6-address*
Описание параметров	*ipv6-address*: указывает IPv6-адрес DNS-сервера
Режим конфигурации	Режим конфигурации пула DHCPv6
Встроенная подсказка	Для настройки нескольких адресов DNS-серверов можно запустить команду **dns-server** несколько раз. Новый адрес DNS-сервера не перезаписывает старые адреса DNS-серверов

Настройка имен доменов на сервере DHCPv6

Команда	**domain-name** *domain*
Описание параметров	*domain*: определяет имя домена, которое будет выделено пользователю
Режим конфигурации	Режим конфигурации пула DHCPv6
Встроенная подсказка	Чтобы создать несколько доменных имен, можно запустить команду **domain-name** несколько раз. Новое доменное имя не перезаписывает старые доменные имена

Настройка опции 52 на сервере DHCPv6

Команда	**option52** *ipv6-address*
Описание параметров	*ipv6-address*: указывает IPv6-адрес AC CAPWAP
Режим конфигурации	Режим конфигурации пула DHCPv6
Встроенная подсказка	Можно запустить команду **option52** для настройки адресов IPv6 для нескольких CAPWAP AC. Новый адрес CAPWAP AC IPv6 не перезаписывает старые адреса IPv6

Включение службы сервера DHCPv6

Команда	**ipv6 dhcp server** *poolname* **[rapid-commit] [preference** *value***]**
Описание параметров	*poolname*: указывает имя определяемого пользователем пула конфигурации DHCPv6. **rapid-commit:** позволяет выполнять обмен двумя сообщениями. **preference** *value***:** настройка приоритета сообщения advertise в диапазоне от 0 до 255. Значение по умолчанию — 0
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Запустите команду **ipv6 dhcp server**, чтобы включить службу DHCPv6 на интерфейсе. При настройке ключевого слова **rapid-commit** обмен двумя сообщениями с клиентом разрешен во время назначения префиксов адресов и других конфигураций. После настройки этого ключевого слова, если сообщение запроса от клиента содержит параметр **rapid-commit**, сервер DHCPv6 отправит сообщение ответа напрямую. Если для параметра **preference** установлено значение, не равное 0, сообщение advertise, отправленное сервером DHCPv6, содержит параметр настройки. Поле **preference** влияет на выбор сервера клиентом. Если сообщение advertise не содержит этого поля, то значение **preference** считается **0**. Если значение **preference**, полученное клиентом, равно 255, клиент немедленно отправляет на сервер запрос на получение конфигураций. Функции клиента, сервера и ретрансляции DHCPv6 являются взаимоисключающими. Интерфейс может быть настроен только с одной функцией одновременно

5.4.1.6. Пример конфигурации

Настройка сервера DHCPv6

Этапы конфигурации	• Настройте пул конфигурации с именем "pool1". • Настройте префикс адреса IA_NA для сервера DHCPv6. • Настройте префиксы статически привязанных адресов на сервере DHCPv6. • Настройте два DNS-сервера. • Настройте имя домена. • Включите службу сервера DHCPv6 на интерфейсе
	QTECH# configure terminal QTECH(config)# ipv6 dhcp pool pool1 QTECH(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000 QTECH(config-dhcp)#prefix-delegation 2008:2::/64 0003000100d0f82233ac QTECH(config-dhcp)# dns-server 2008:1::1 QTECH(config-dhcp)# dns-server 2008:1::2 QTECH(config-dhcp)# domain-name example.com QTECH(config-dhcp)#exit QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if)# ipv6 dhcp server pool1
Проверка конфигурации	• Запустите команду **show ipv6 dhcp pool**, чтобы отобразить созданный пул конфигурации
	QTECH# show ipv6 dhcp pool DHCPv6 pool: pool1 Static bindings: Binding for client 0003000100d0f82233ac IA PD prefix: 2008:2::/64 preferred lifetime 3600, valid lifetime 3600 IANA address range: 2008:50::1/64 -> 2008:50::ffff:ffff:ffff:ffff/64 preferred lifetime 1000, valid lifetime 2000 DNS server: 2008:1::1 DNS server: 2008:1::2 Domain name: example.com

5.4.1.7. Типичные ошибки

- Указанное имя пула слишком длинное.
- Количество пулов конфигурации превышает системное ограничение (256).
- Конфигурация выполняется на других интерфейсах, кроме интерфейса коммутатора Virtual Interface (SVI), маршрутизируемого порта и агрегированного порта L3.
- Количество интерфейсов, настроенных со службой сервера DHCPv6, превышает системное ограничение (256).
- Указанное значение срока службы **valid lifetime** меньше значения предпочтительного срока службы **preferred lifetime**.
- Указан недопустимый адрес IA_NA.
- Количество диапазонов адресов превышает системное ограничение (20).
- При настройке префиксов статически привязанных адресов указанные идентификаторы DUID слишком длинные.
- Количество префиксов статически привязанных адресов превышает системное ограничение (1024).
- Если настроен локальный пул префиксов, указанное значение срока службы **valid lifetime** меньше значения предпочтительного срока службы **preferred lifetime**.
- Количество DNS-серверов превышает системное ограничение (10).
- Количество имен доменов превышает системное ограничение (10).
- Количество адресов option52 превышает системное ограничение (10).

5.4.2. Настройка DHCPv6 Relay

5.4.2.1. Результат конфигурации

Агент ретрансляции DHCPv6 может быть настроен на распределение адресов, делегирование префиксов и распределение параметров, чтобы обеспечить связь между клиентом DHCPv6 и сервером по различным каналам.

5.4.2.2. Примечания

Необходимо указать адрес назначения. Если адрес назначения является адресом многоадресной рассылки (например, FF05::1:3), необходимо также указать интерфейс выхода.

5.4.2.3. Этапы конфигурации

Настройка функции агента ретрансляции DHCPv6

- Обязательно.
- Если не указано иное, необходимо настроить функцию агента ретрансляции DHCPv6 на всех устройствах, которым требуется обеспечить службу агента ретрансляции DHCPv6.

5.4.2.4. Проверка конфигурации

- Клиент DHCPv6 и сервер DHCPv6 обмениваются сообщениями через агента ретрансляции.
- Проверьте, включен ли интерфейс с помощью реле DHCPv6.

- Проверьте, может ли агент ретрансляции DHCPv6 получать и отправлять сообщения.

5.4.2.5. Связанные команды

Настройка функции агента ретрансляции DHCPv6

Команда	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interfacenumber*]
Описание параметров	*ipv6-address*: указывает адрес назначения оператора ретрансляции. *interface-type*: указывает тип интерфейса назначения (необязательно). *interface-number*: указывает номер интерфейса назначения (необязательно)
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Все пакеты DHCPv6 от клиентов, полученные интерфейсом, активированным функцией ретрансляции DHCPv6, инкапсулируются и отправляются по указанному адресу назначения (или нескольким адресам назначения) через указанный интерфейс (ОПЦИОНАЛЬНО)

5.4.2.6. Пример конфигурации

Настройка DHCPv6 Relay

Этапы конфигурации	Укажите интерфейс, включенный службой ретрансляции для пересылки полученных пакетов клиента DHCPv6 на указанный адрес назначения через указанный интерфейс (необязательно)
	QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#interface vlan 1 QTECH(config-if)#ipv6 dhcp relay destination 3001::2 QTECH(config-if)#ipv6 dhcp relay destination ff02::1:2 vlan 2
Проверка конфигурации	Выполните команду **show ipv6 dhcp relay destination all**, чтобы отобразить настроенные адреса назначения
	Interface:VLAN 1 Destination address(es) Output Interface 3001::2 ff02::1:2 VLAN 2

5.4.2.7. Типичные ошибки

Конфигурация выполняется на других интерфейсах, кроме интерфейса коммутатора Virtual Interface (SVI), маршрутизируемого порта и порта точки доступа L3.

5.5. Контроль состояния

5.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и, следовательно, прерыванию работы служб.

Описание	Команда
Очищает привязки DHCPv6	**clear ipv6 dhcp binding** [*ipv6-address*]
Очищает статистику сервера DHCPv6	**clear ipv6 dhcp server statistics**
Удаляет конфликтующие адреса на сервере DHCPv6	**clear ipv6 dhcp conflict** { *ipv6-address* | * }
Удаляет статистику отправленных и полученных пакетов после включения на текущем устройстве ретрансляции DHCPv6	**clear ipv6 dhcp relay statistics**

5.5.2. Отображение

Описание	Команда
Отображает DUID устройства	**show ipv6 dhcp**
Отображает привязку адресов на сервере DHCPv6	**show ipv6 dhcp binding** [*ipv6-address*]
Отображает интерфейс DHCPv6	**show ipv6 dhcp interface** [*interface-name*]
Отображает пул DHCPv6	**show ipv6 dhcp pool** [*poolname*]
Отображает конфликтующие адреса DHCPv6	**show ipv6 dhcp conflict**
Отображает статистику на сервере DHCPv6	**show ipv6 dhcp server statistics**

Описание	Команда
Отображает адрес назначения агента ретрансляции DHCPv6	**show ipv6 dhcp relay destination** { **all** | *interface-type interface-number* }
Отображает статистику отправленных и полученных пакетов после включения на устройстве реле DHCPv6	**show ipv6 dhcp relay statistics**
Отображает локальный пул префиксов IPv6	**show ipv6 local pool** [*poolname*]

5.5.2.1. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Отладка DHCPv6	**debug ipv6 dhcp** [**detail**]

6. НАСТРОЙКА DNS

6.1. Обзор

Система доменных имен (DNS) — это распределенная база данных, содержащая сопоставления между доменными именами и IP-адресами в Интернете, что облегчает пользователям доступ в Интернет без необходимости запоминать IP-адреса, доступ к которым напрямую осуществляется компьютерами. Процесс получения IP-адреса через соответствующее имя хоста называется разрешением имени домена (или разрешением имени хоста).

6.1.1. Протоколы и стандарты

- RFC1034: доменные имена — понятия и возможности.
- RFC1035: доменные имена — реализация и спецификация.

6.2. Применение

Применение	Описание
Статическое разрешение доменного имени	Разрешение доменных имен выполняется непосредственно на основе сопоставления имени домена и IP-адреса устройства
Динамическое разрешение доменного имени	Динамически получает IP-адрес, сопоставленный с доменным именем, от DNS-сервера в сети

6.2.1. Статическое разрешение доменного имени

6.2.1.1. Сценарий

- Предварительно задайте соответствие между именем домена и IP-адресом устройства.
- При выполнении операций с доменными именами (например, Ping и Telnet) с помощью прикладных программ, система может разрешить IP-адрес без подключения к серверу в сети.

6.2.1.2. Описание

Предварительно задайте соответствие между именем домена и IP-адресом устройства.

6.2.2. Динамическое разрешение доменного имени

6.2.2.1. Сценарий

- DNS-сервер развернут в сети для предоставления службы доменных имен.
- Имя домена "host.com" развернуто в сети.
- Устройство-A применяется к DNS-серверу для имени домена "host.com".

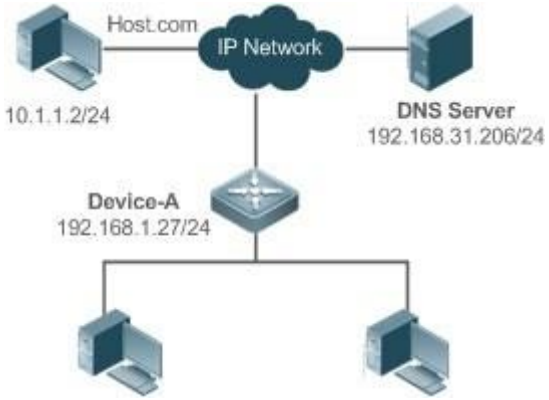


Рисунок 6-1. Динамическое разрешение имени домена

6.2.3. Развертывания

Разверните DNS-сервер в качестве DNS-сервера устройства A.

6.3. Ключевые особенности

6.3.1. Базовые концепции

DNS

DNS состоит из преобразователя и DNS-сервера. DNS-сервер хранит сопоставления имен доменов и IP-адресов всех узлов в сети и реализует взаимное преобразование имен доменов и IP-адресов. Идентификаторы портов TCP и UDP DNS имеют значение 53, и обычно используется порт UDP.

6.3.2. Ключевые особенности

Функция	Описание
Разрешение имени домена	IP-адреса получаются на основе доменных имен с DNS-сервера или локальной базы данных

6.3.3. Разрешение имени домена

6.3.3.1. Принцип работы

Разрешение статического имени домена

Статическое разрешение имени домена означает, что пользователь предварительно задает соответствие между именем домена и IP-адресом на устройстве. При выполнении операций с доменными именами (например, Ping и Telnet) с помощью прикладных программ, система может разрешить IP-адрес без подключения к серверу в сети.

Динамическое разрешение имени домена

Динамическое разрешение доменных имен означает, что при выполнении пользователем операций с доменными именами через прикладные программы преобразователь DNS-системы запрашивает у внешнего DNS-сервера IP-адрес, сопоставленный с доменным именем.

Процедура динамического разрешения доменных имен:

1. Пользовательская прикладная программа (например, Ping или Telnet) запрашивает IP-адрес, сопоставленный с доменным именем, из DNS-преобразователя системы.
   - Преобразователь DNS сначала запрашивает динамический кеш. Если имя домена в динамическом кеше не истекло, DNS-преобразователь возвращает имя домена в приложение.
   - Если срок действия всех доменных имен истекает, DNS-преобразователь инициирует запрос на преобразование доменных имен IP-адресов во внешний DNS-сервер.
2. После получения ответа от DNS-сервера, DNS-преобразователь кеширует и передает ответ приложению.

6.3.3.2. Связанная конфигурация

Включение разрешения имени домена

- По умолчанию разрешение доменных имен включено.
- Запустите команду поиска **ip domain-lookup**, чтобы включить или отключить разрешение имени домена.

Настройка IP-адреса, сопоставленного с статическим доменным именем

- По умолчанию не настроено сопоставление имени домена и IP-адреса.
- Выполните команду **ip host**, чтобы указать IPv4-адрес, сопоставленный с доменным именем.

Настройка DNS-сервера

- По умолчанию DNS-сервер не настроен.
- Выполните команду **ip name-server**, чтобы настроить DNS-сервер.

6.4. Настройка

Настройка	Описание и команда	
Настройка статического разрешения доменного имени	Опционально	
	ip domain-lookup	Включение разрешения доменных имен
	ip host	Настройка адреса IPv4, сопоставленного с именем домена
Настройка динамического разрешения доменного имени	Опционально	
	ip domain-lookup	Включение разрешения доменных имен
	ip name-server	Конфигурирует DNS-сервер

6.4.1. Настройка статического разрешения доменного имени

6.4.1.1. Результат конфигурации

Средство выделения сигнала системы разрешает IP-адрес, сопоставленный с именем домена на локальном устройстве.

6.4.1.2. Этапы конфигурации

Включение разрешения имени домена

- Функция разрешения имени домена включена по умолчанию.
- Если эта функция отключена, разрешение статического имени домена не вступает в силу.

Настройка адреса IPv4, сопоставленного с именем домена

(Обязательно) используемые доменные имена должны быть настроены с привязанным IP-адресом.

6.4.1.3. Проверка конфигурации

- Выполните команду **show running** для проверки конфигураций.
- Выполните команду **show hosts**, чтобы проверить соответствие между именем домена и IP-адресом.

6.4.1.4. Связанные команды

Настройка адреса IPv4, сопоставленного с именем домена

Команда	**ip host** *host-name ip-address*
Описание параметров	*host-name*: указывает имя домена. *ip-address*: указывает сопоставленный IPv4-адрес
Режим конфигурации	Режим глобальной конфигурации

6.4.1.5. Пример конфигурации

Настройка разрешения статического имени домена

Этапы конфигурации	Установите IP-адрес статического доменного имени www.test.com на 192.168.1.1 на устройстве
	QTECH#configure terminal QTECH(config)# ip host www.test.com 192.168.1.1 QTECH(config)# exit
Проверка конфигурации	Выполните команду **show hosts**, чтобы проверить, настроена ли запись статического имени домена

	QTECH#show hosts Name servers are: Host type Address TTL(sec) www.test.com static 192.168.1.1 ---

6.4.2. Настройка динамического разрешения доменного имени

6.4.2.1. Результат конфигурации

Преобразователь системы разрешает IP-адрес, сопоставленный с доменным именем через DNS-сервер.

6.4.2.2. Этапы конфигурации

Включение разрешения имени домена

- Разрешение имени домена включено по умолчанию.
- Если эта функция отключена, динамическое разрешение доменных имен не вступает в силу.

Настройка DNS-сервера

(Обязательно) чтобы использовать динамическое разрешение имен доменов, необходимо настроить внешний DNS-сервер.

6.4.2.3. Проверка конфигурации

Выполните команду **show running** для проверки конфигураций.

6.4.2.4. Связанные команды

Настройка DNS-сервера

Команда	**ip name-server** [**oob**] *ip-address* [**via** mgmt-name]
Описание параметров	*ip-address*: указывает IPv4-адрес DNS-сервера. **oob**: указывает, что DNS-сервер доступен через внеполосный интерфейс управления (интерфейс управления). ***via**:* настройка интерфейса управления выходом. *mgmt-name:* указывает интерфейс управления исходными вызовами для пакетов в режиме oob
Режим конфигурации	Режим глобальной конфигурации

6.4.2.5. Пример конфигурации

Настройка динамического разрешения имени домена

Сценарий

Рисунок 6-2.

Устройство разрешает доменное имя через DNS-сервер (192.168.10.1) в сети.

Этапы конфигурации	Установите IP-адрес DNS-сервера на устройстве равным 192.168.10.1
	DEVICE#configure terminal DEVICE(config)# ip name-server 192.168.10.1 DEVICE(config)# exit
Проверка конфигурации	Запустите команду **show hosts**, чтобы проверить, указан ли DNS-сервер
	QTECH(config)#show hosts Name servers are: 192.168.10.1 static Host type Address TTL(sec)

6.5. Контроль состояния

6.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команды очистки во время работы устройства может привести к потере данных или даже прерыванию служб.

Описание	Команда
Очищает таблицу кеша динамических имен хостов	**clear host** [*host-name*]

6.5.2. Отображение

Описание	Команда
Отображение параметров DNS	**show hosts** [*host-name*]

6.5.3. Отладка

ПРИМЕЧАНИЕ: системные ресурсы используются при выводе отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Отладка функции DNS	**debug ip dns**

7. НАСТРОЙКА СЕРВЕРА FTP

7.1. Обзор

Функционал позволяет устройству выполнять функции FTP-сервера. Таким образом, пользователь может подключить FTP-клиент к FTP-серверу и загрузить файлы по протоколу FTP.

Пользователь может использовать функционал FTP-сервера для простого получения файлов, таких как файлы syslog, с устройства и копирования файлов в файловую систему устройства по протоколу FTP.

7.1.1. Протоколы и стандарты

- RFC959: протокол передачи файлов (FTP).
- RFC3659: расширения для FTP.
- RFC2228: расширения безопасности FTP.
- RFC2428: расширения FTP для IPv6 и NAT.
- RFC1635: как использовать анонимный FTP.

7.2. Применение

Применение	Описание
Предоставление службы FTP в локальной сети	Предоставляет службы загрузки и загрузки для пользователя в локальной сети (LAN)

7.2.1. Предоставление службы FTP в локальной сети

7.2.1.1. Сценарий

Предоставление услуг загрузки и скачивания для пользователя в локальной сети.

Как показано на Рисунке 7-1, FTP-сервер включен в локальной сети.

- На G и S включен функционал FTP-сервера.
- Пользователь инициирует запрос на загрузку по протоколу FTP.

Рисунок 7-1.

G — это шлюз.

S — это коммутатор.

7.2.1.2. Описание

- На G включается функционал FTP-сервера.
- Как коммутатор уровня 2, S обеспечивает функцию прозрачной передачи на 2 уровне.

7.3. Ключевые особенности

7.3.1. Базовые концепции

FTP

FTP — это стандартный протокол, определенный сетевой рабочей группой IETF. Он реализует передачу файлов на основе протокола управления передачей (TCP). FTP позволяет пользователю передавать файлы между двумя сетевыми компьютерами и является распространенным способом передачи файлов в Интернете. Кроме того, FTP предоставляет такие функции, как вход в систему, запрос по каталогу, работа с файлами и другие функции управления сеансом. Среди семейства протоколов TCP/IP FTP является протоколом прикладного уровня и использует порты TCP 20 и 21 для передачи. Порт 20 используется для передачи данных, а порт 21 используется для передачи управляющих сообщений. Основные операции FTP описаны в RFC959.

Авторизация пользователя

Для подключения FTP-клиента к FTP-серверу необходимо иметь учетную запись, разрешенную FTP-сервером. То есть, пользователь может пользоваться услугами, предоставляемыми FTP-сервером после входа на FTP-сервер с именем пользователя и паролем.

Режимы передачи файлов FTP

FTP поддерживает два режима передачи файлов:

- Режим передачи текста (режим ASCII): Он используется для передачи текстовых файлов (например, файлов .txt, .bat и .cfg). Этот режим отличается от двоичного режима при обработке возврата каретки и перевода строки. В режиме ASCII возврат каретки и строка сменяются на локальные символы CRC, например, \n в Unix, \r\n в Windows и \r в Mac. Предположим, что копируемый файл содержит текст ASCII. Если удаленный компьютер не работает под управлением Unix, FTP автоматически преобразует формат файла в соответствии с требованиями удаленного компьютера.
- Двоичный режим передачи: Он используется для передачи программных файлов (например, файлов .app, .bin и. btm), включая исполняемые файлы, сжатые файлы и файлы изображений без обработки данных. Таким образом, двоичный режим обеспечивает более быструю передачу всех файлов и более надежную передачу файлов ASCII.

Рабочие режимы FTP

FTP обеспечивает два рабочих режима:

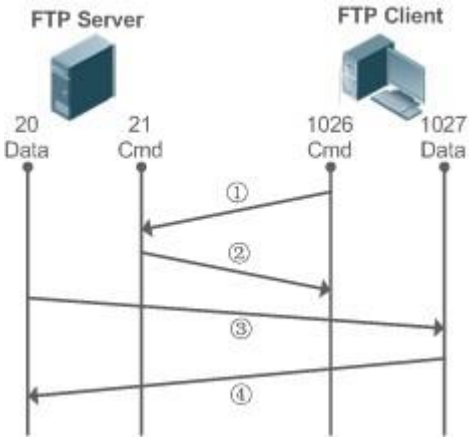


Рисунок 7-2.

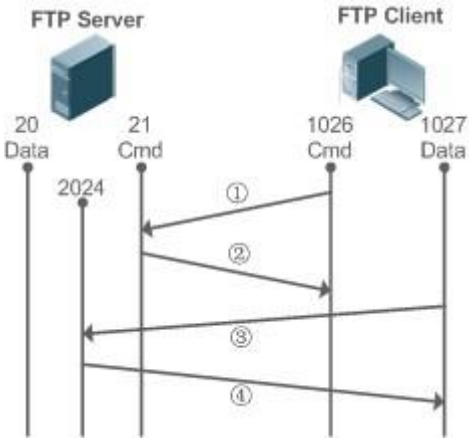


Рисунок 7-3.

- Рисунок 7-2 показывает активный режим (PORT). FTP-клиент использует порт 1026 для подключения к FTP-серверу через порт 21. Клиент отправляет команды через этот канал. Перед получением данных клиент отправляет команду **PORT** на этом канале. Команда **PORT** содержит информацию о порте канала (1027) клиента для получения данных. Сервер использует порт 20 для подключения к клиенту через порт 1027 для создания канала данных для приема и передачи данных. FTP-сервер должен установить новое соединение с клиентом для передачи данных.
- Рисунок 7-3 показывает пассивный режим (PASV). Процесс создания управляющего канала аналогичен процессу в режиме PORT. Однако после установления соединения клиент отправляет команду **PASV**, а не команду **PORT**. После получения команды **PASV** FTP-сервер включает порт высшего класса (2024) в случайном порядке и уведомляет клиента о том, что данные будут переданы на этот порт. Клиент использует порт 1027 для подключения FTP-сервера через порт 2024. Затем клиент и сервер могут передавать и принимать данные по этому каналу. В этом случае FTP-серверу не нужно устанавливать новое соединение с клиентом.

Поддерживаемые команды FTP

После получения запроса на подключение по протоколу FTP сервер FTP требует от клиента предоставить имя пользователя и пароль для аутентификации.

Если клиент проходит проверку подлинности, команды FTP-клиента могут быть выполнены для операций. Доступные команды FTP-клиента перечислены ниже:

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye		mget		rename	system
cd	get	mkdir	passive		type
cdup		mls	put	rmdir	user
close	ls		pwd		

Для получения информации об использовании этих команд FTP-клиента см. документ по FTP-клиенту. Кроме того, многие клиентские инструменты FTP (такие как CuteFTP и FlashFXP) поддерживают графический интерфейс пользователя. Эти инструменты упрощают операции, освобождая пользователей от настройки команд FTP.

7.3.2. Обзор

Функция	Описание
Включение функции FTP-сервера	Предоставляет функции загрузки, скачивания, отображения, создания и удаления файлов для клиента FTP

7.3.3. Включение функции FTP-сервера

7.3.3.1. Принцип работы

Основной принцип работы описан в предыдущей главе. Устройства QTECH предоставляют службы FTP после настройки имени пользователя, пароля и каталога верхнего уровня.

7.3.3.2. Связанная конфигурация

Включение функции FTP-сервера в глобальном масштабе Функция FTP-сервера по умолчанию отключена.

Запустите команду **ftp-server enable**, чтобы включить функцию FTP-сервера.

Перед использованием FTP-сервера необходимо включить его глобально.

Настройка имени пользователя, пароля и каталога верхнего уровня

По умолчанию нет авторизованного пользователя или каталога верхнего уровня.

Запустите команды **ftp-server password**, **ftp-server username** и **ftp-server topdir**, чтобы установить авторизированный пользователь и каталог верхнего уровня.

Три вышеперечисленные конфигурации являются обязательными; в противном случае функционал FTP-сервера не может быть включен.

7.4. Настройка

Настройка	Описание и команда	
Настройка основных функций	(Обязательно) он используется для включения FTP-сервера	
	ftp-server enable	Включает функцию FTP-сервера
	ftp-server login timeout	Настройка тайм-аута входа для сеанса FTP
	ftp-server login times	Настройка допустимого количества входов в систему
	ftp-server topdir *directory*	Настройка каталога верхнего уровня FTP-сервера
	ftp-server username *username*	Настройка имени пользователя
	ftp-server password [*type*] *password*	Настройка пароля
	Опционально	
	ftp-server timeout *time*	Настройка тайм-аута простоя FTP-сеанса

7.4.1. Настройка основных функций

7.4.1.1. Результат конфигурации

Создайте FTP-сервер, чтобы предоставить FTP-службы для FTP-клиента.

7.4.1.2. Примечания

- Необходимо настроить имя пользователя, пароль и каталог верхнего уровня.
- Чтобы сервер закрыл нестандартную сессию в течение ограниченного периода времени, необходимо настроить тайм-аут простоя сессии.

7.4.1.3. Этапы конфигурации

Включение функции FTP-сервера

- Обязательно.
- Если не указано иное, включите функцию FTP-сервера на каждом маршрутизаторе.

Настройка каталога верхнего уровня

- Обязательно.
- Если не указано иное, настройте директорию верхнего уровня в качестве корневого каталога на каждом маршрутизаторе.

Настройка имени пользователя и пароля для входа в систему

- Обязательно.
- Длина имени пользователя и пароля ограничена.

Настройка времени ожидания входа для сеанса FTP

- Опционально.
- Если клиент отключен от сервера из-за ошибки или других нештатных причин, FTP-сервер может не знать, что пользователь отключен и продолжает поддерживать соединение. Следовательно, FTP-соединение занято на длительное время, и сервер не может отвечать на запросы входа других пользователей. Эта конфигурация может гарантировать, что другие пользователи смогут подключиться к FTP-серверу в течение определенного периода времени при возникновении ошибки.

7.4.1.4. Проверка конфигурации

Подключите FTP-клиент к FTP-серверу.

- Проверьте, подключен ли клиент.
- Проверьте, нормально ли работают операции на клиенте.

7.4.1.5. Связанные команды

Включение функции FTP-сервера

Команда	**ftp-server enable**
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Клиент не может получить доступ к FTP-серверу, если не настроен верхний уровень каталога, имени пользователя и пароля. Поэтому рекомендуется настроить верхний уровень каталога, имени пользователя и пароля для входа в систему, обратившись к последующим главам перед первым включением службы

Настройка допустимого количества регистраций

Команда	**ftp-server login times** *times*
Описание параметров	*times:* указывает допустимое количество входов в систему в диапазоне от 1 до 10
Режим конфигурации	Режим глобальной конфигурации

Встроенная подсказка	Допустимое количество входов соответствует количеству попыток проверки учетных записей во время сеанса FTP. Значение по умолчанию — 3, что означает, что сеанс будет прерван, если вы введете неверное имя пользователя или пароль три раза, и другие пользователи смогут перейти в оперативный режим

Настройка времени ожидания входа для сеанса FTP

Команда	**ftp-server login timeout** *timeout*
Описание параметров	*timeout*: указывает время ожидания входа в систему в диапазоне от 1 до 30 минут
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Тайм-аут входа означает максимальную продолжительность сеанса с момента его создания. Если вы не пройдете повторную проверку пароля во время тайм-аута входа в систему, сеанс будет прерван, чтобы другие пользователи могли войти в систему

Настройка каталога верхнего уровня FTP-сервера

Команда	**ftp-servertopdir** *directory*
Описание параметров	*directory:* указывает путь доступа пользователя
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Если верхний каталог сервера установлен на "/syslog", FTP-клиент может получить доступ только к файлам и каталогам в каталоге "/syslog" на устройстве после входа в систему. Из-за ограничений в каталоге верхнего уровня клиент не может попасть в каталог выше, чем "/syslog"

Настройка имени пользователя для входа на сервер

Команда	**ftp-server username** *username*
Описание параметров	*username* (Имя пользователя): указывает имя пользователя
Режим конфигурации	Режим глобальной конфигурации

Встроенная подсказка	FTP-сервер не поддерживает анонимный вход в систему, поэтому необходимо настроить имя пользователя. Имя пользователя состоит из 64 символов, включая буквы, цифры и символы без пробелов

Настройка имени пользователя и пароля для входа на сервер

Команда	**ftp-server password** [*type*] *password*
Описание параметров	*type*: 0 или 7. 0 означает, что пароль не зашифрован (в виде открытого текста), а 7 указывает на то, что пароль зашифрован (текст шифра). **password**: указывает пароль
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Пароль состоит только из букв или цифр. Пробелы в начале и конце пароля игнорируются. Пробелы внутри пароля рассматриваются как часть пароля. Пароль в виде простого текста состоит из 1–25 символов. Пароль для шифрования состоит из 4–52 символов. Имена пользователей и пароли должны совпадать. Можно настроить не более 10 пользователей

Настройка тайм-аута простоя для сеанса FTP

Команда	**ftp-Server timeout** *time*
Описание параметров	*time*: указывает время ожидания простоя в диапазоне от 1 до 3600 минут
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Тайм-аут простоя сеанса относится к продолжительности от окончания операции FTP до начала следующей операции в сеансе FTP. После того, как сервер отвечает на команду FTP-клиента (например, после полной передачи файла), сервер начинает отсчет времени простоя и останавливается при получении следующей команды FTP-клиента. Поэтому настройка тайм-аута простоя не влияет на некоторые трудоемкие операции передачи файлов

Отображение состояния сервера

Команда	**show ftp-server**
Режим конфигурации	Привилегированный EXEC режим
Встроенная подсказка	Выполните эту команду, чтобы отобразить состояние FTP-сервера

Отладка

Команда	**debug ftp-server pro/err**
Режим конфигурации	Привилегированный EXEC-режим
Встроенная подсказка	Выполните эту команду, чтобы отлаживать сообщения/ошибки FTP-сервера

7.4.1.6. Пример конфигурации

Создание FTP-сервера в сети IPv4

Этапы конфигурации	• Включает функцию сервера FTP. • Настройте каталог/системный журнал верхнего уровня. • Установите имя пользователя на user и пароль на password. • Установите для тайм-аута простоя сеанса значение 5 минут
	QTECH(config)#ftp-server username user QTECH(config)#ftp-server password password QTECH(config)#ftp-server timeout 300 QTECH(config)#ftp-server topdir / QTECH(config)#ftp-server enable
Проверка конфигурации	• Выполните команду **show ftp-server**, чтобы проверить результат

```
QTECH#show ftp-server
  ftp-server information
==================================
enable : Y
topdir : /
timeout: 30min
username config : Y
password config : Y
transfer type: ASCII
control connection : N
port data connection : N
passive data connection : N
QTECH#
```

7.4.1.7. Типичные ошибки

- Имя пользователя не настроено.
- Пароль не настроен.
- Каталог верхнего уровня не настроен.

7.5. Контроль состояния

7.5.1. Отображение

Описание	Команда
Отображает конфигурацию FTP-сервера	**show ftp-server**

7.5.2. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Отладка событий ошибок FTP-сервера	**debug ftp-server err**
Отладка событий сообщений FTP-сервера	**debug ftp-server pro**

8. НАСТРОЙКА КЛИЕНТА FTP

8.1. Обзор

Протокол передачи файлов (FTP) является приложением TCP/IP. Установив надежное и соединение TCP между FTP-клиентом и сервером, пользователь может получить доступ к удаленному компьютеру, на котором запущен FTP-сервер.

Клиент FTP обеспечивает передачу файлов между устройством и FTP-сервером по протоколу FTP. Пользователь использует клиент для отправки команды на сервер. Сервер отвечает на команду и отправляет результат выполнения клиенту. С помощью командного взаимодействия пользователь может просматривать файлы в каталоге сервера, копировать файлы с удаленного компьютера на локальный компьютер или передавать локальные файлы на удаленный компьютер.

Протокол FTP предназначен для облегчения обмена файлами программ/данных и поощрения удаленной работы (с помощью программ). Пользователям не нужно беспокоиться о различиях между различными системами файлов на разных хостах. Данные передаются эффективным и надежным образом. FTP обеспечивает безопасное удаленное управление файлами.

FTP-клиенты QTECH отличаются от стандартных FTP-клиентов, которые работают с интерактивными командами. Вместо этого введите команду **copy** в интерфейсе командной строки, чтобы выполнить инструкции по подключению управления, такие как **open**, **user** и **pass**. После установки управляющего соединения начинается процесс передачи файлов, а затем устанавливается соединение для передачи или загрузки файлов.

8.1.1. Протоколы и стандарты

RFC959: протокол передачи файлов (FTP).

8.2. Применение

Применение	Описание
Загрузка локального файла на удаленный сервер	Локальные и удаленные файлы должны быть переданы, например, для загрузки локального файла на удаленный сервер
Загрузка файла с удаленного сервера на локальное устройство	Локальные и удаленные файлы должны быть переданы, например, для загрузки файла с удаленного сервера на локальное устройство

8.2.1. Загрузка локального файла на удаленный сервер

8.2.1.1. Сценарий

Локальные и удаленные файлы должны быть переданы, например, для загрузки локального файла на удаленный сервер.

Как показано на Рисунке 8-1, ресурсы используются только в сети.

Рисунок 8-1.

8.2.1.2. Описание

- Включите загрузку файлов на FTP-клиенте.
- Включите загрузку файлов на FTP-сервер.

8.2.2. Загрузка файла с удаленного сервера на локальное устройство

8.2.2.1. Сценарий

Локальные и удаленные файлы должны быть переданы, например, для загрузки файла с удаленного сервера на локальное устройство.

Как показано на Рисунке 8-2, ресурсы используются только в сети.

Рисунок 8-2.

8.2.2.2. Описание

- Включите загрузку файлов на FTP-клиенте.
- Включите загрузку файлов на FTP-сервере.

8.3. Ключевые особенности

8.3.1. Базовые концепции

Загрузка файлов FTP

Загрузка файлов с FTP-клиента на FTP-сервер.

Скачивание файлов FTP

Загрузка файлов с FTP-сервера на FTP-клиент.

Режим подключения FTP

FTP-клиент и FTP-сервер могут быть подключены в активном или пассивном режиме.

Режим передачи по FTP

Передача данных между FTP-клиентом и FTP-сервером возможна в двух режимах: в текстовом (ASCII) и двоичном (двоичном).

Указание IP-адреса интерфейса источника для передачи по FTP

Клиент FTP настроен на использование исходного IP-адреса для связи с FTP-сервером.

8.3.2. Обзор

Функция	Описание
Загрузка файлов FTP	Загрузка файлов с FTP-клиента на FTP-сервер
Скачивание файлов FTP	Загрузка файлов с FTP-сервера на FTP-клиент
Режим подключения FTP	Указывает режим соединения между FTP-клиентом и FTP-сервером
Режим передачи по FTP	Указывает режим передачи между FTP-клиентом и FTP-сервером
Указание IP-адреса интерфейса источника для передачи по FTP	Настройка исходного IP-адреса FTP-клиента для связи с FTP-сервером

8.3.3. Загрузка файлов FTP

FTP позволяет загружать файлы. Запустите FTP-клиент и FTP-сервер одновременно и загрузите файлы с FTP-клиента на FTP-сервер.

8.3.4. Скачивание файлов FTP

FTP позволяет скачивать файлы. Запустите FTP-клиент и FTP-сервер одновременно и загрузите файлы с FTP-сервера на FTP-клиент.

8.3.5. Режим подключения FTP

FTP должен использовать два соединения TCP: один канал управления (командное соединение), который используется для передачи команд между FTP-клиентом и сервером; другой канал передачи данных используется для передачи или загрузки данных.

Соединение управления: Некоторые простые сеансы доступны только с управляющим подключением. Клиент отправляет команду на сервер. После получения команды сервер отправляет ответ. (Рисунок 8-3).

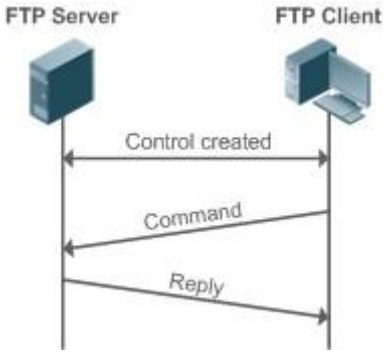


Рисунок 8-3.

Соединение управления и передача данных: Когда клиент отправляет команду на загрузку или загрузку данных, необходимо установить, как управляющее соединение, так и соединение для передачи данных.

FTP поддерживает два режима передачи данных: активный (PORT) и пассивный (PASC). При установлении соединения для передачи данных используются разные режимы.

- Активный режим

В этом режиме FTP-сервер активно подключается к FTP-клиенту при установлении соединения для передачи данных. Этот режим состоит из четырех этапов:

Клиент использует исходный порт 5150 для связи с сервером через порт 21, как показано на Рисунке 8-4, чтобы отправить запрос на подключение и сообщить серверу, что используемый порт — порт 5151.

После получения запроса сервер отправляет ответ OK (ACK). Обмен данными между клиентом и сервером управляет сигнализацией через консольные порты.

Сервер позволяет порту 20 в качестве исходного порта отправлять данные на порт 5151 клиента.

Клиент отправляет ответ. Передача данных завершается.

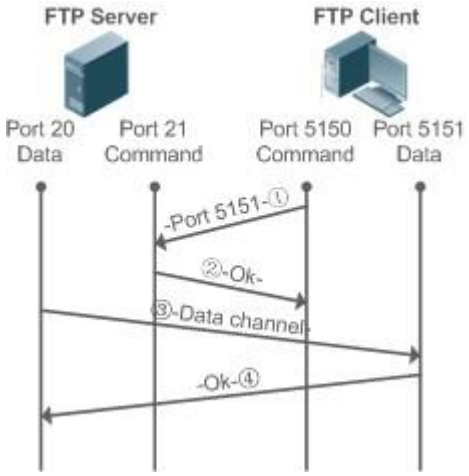


Рисунок 8-4. Активный режим (PORT)

- Пассивный режим

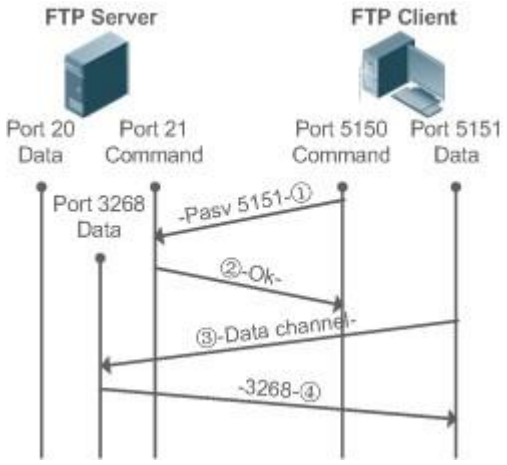


Рисунок 8-5. Пассивный режим (PASV)

Этот режим часто задается командой **passive**. После установления соединения для передачи данных FTP-сервер подключается к клиенту FPT пассивно. Этот режим состоит из четырех этапов:

В пассивном режиме клиент инициализирует сигнальное соединение управления. Клиент использует исходный порт 5150 для подключения к серверу через порт 21, как показано на Рисунке 8-5, и запускает команду **passive**, чтобы запросить переход сервера в режим PASV.

Сервер соглашается войти в режим PASV, выбирает номер порта, превышающий 1024, случайным образом и сообщает номер порта клиенту.

После получения сообщения клиент использует порт 5151, как показано на рис. 15, для связи с сервером через порт 3268. Здесь порт 5151 является исходным портом, а порт 3268 — портом назначения.

После получения сообщения сервер отправляет данные и отвечает ACK (OK).

После установления соединения для передачи данных можно выполнить загрузку и скачивание файлов. Кроме того, можно выполнить некоторые операции с файлом сервера из клиента.

ПРИМЕЧАНИЕ: соединение управления для передачи команд и обратной связи всегда присутствует, тогда как соединение для передачи данных установлено по мере необходимости. Только клиент FTP имеет право выбирать и устанавливать режим PASV или PORT. FTP-клиент отправляет команду для установления соединения с данными. FTP-клиенты QTECH по умолчанию используют режим PASV.

8.3.6. Режим передачи по FTP

FTP предоставляет два режима передачи: текстовый (ASCII) и двоичный (Binary). В настоящее время FTP-клиенты QTECH поддерживают как ASCII, так и двоичный режимы и по умолчанию используют режим BINARY.

- Режим ASCII

Различие между режимами ASCII и Binary заключается в обработке возврата каретки и перевода строки. В режиме ASCII возврат каретки и перевод строки изменяются на локальный символ возврата каретки (CRC), например, \n в Unix, \r\n в Windows и \r в Mac.

- Двоичный режим

Двоичный режим может использоваться для передачи исполняемых файлов, сжатых файлов и файлов изображений без обработки данных. Например, текстовый файл необходимо перенести из Unix в Windows. При использовании двоичного режима разрыв строки в Unix не будет преобразован из \r в \r\n; поэтому в Windows этот файл не имеет строк и отображает много черных квадратов. Таким образом, двоичный режим обеспечивает более быструю передачу всех файлов и более надежную передачу файлов ASCII.

8.3.7. Указание IP-адреса интерфейса источника для передачи по FTP

Клиент FTP настроен на использование исходного IP-адреса для связи с FTP-сервером. Таким образом, клиент FTP подключается к серверу и совместно использует файлы с сервером по указанному исходному IP-адресу.

8.4. Настройка

Настройка	Описание и команда	
Настройка основных функций	(Обязательно) используется для настройки функций FTP-клиента	
	copy flash	Загрузка файла
	copy ftp	Скачивание файла
Настройка дополнительных функций	(ОПЦИОНАЛЬНО) используется для настройки рабочего режима FTP-клиента	
	ftp-client port	Устанавливает режим подключения на активный (port)
	ftp-client ascii	Устанавливает режим передачи ASCII
	ftp-client source-address	Настраивает исходный IP-адрес клиента FTP
	default ftp-client	Восстанавливает настройки по умолчанию, а именно, режим подключения установлен на пассивный (PASV), режим передачи на двоичный и исходный IP-адрес удален

8.4.1. Настройка основных функций

8.4.1.1. Результат конфигурации

Реализация загрузки и скачивания файлов.

8.4.1.2. Примечания

Обратите внимание на форматы команд для загрузки и скачивания.

8.4.1.3. Этапы конфигурации

Загрузка файла

- Эта конфигурация является обязательной, если необходимо загрузить файл.
- Настройте URL-адрес FTP в качестве адреса назначения команды **copy** в привилегированном режиме EXEC.

Скачивание файла

- Эта конфигурация является обязательной при загрузке файла.
- Настройте URL-адрес FTP в качестве адреса источника команды **copy** в привилегированном режиме EXEC.

8.4.1.4. Проверка конфигурации

- Проверьте, существует ли загруженный файл на FTP-сервере.
- Проверьте, существует ли загруженный файл по адресу назначения.

8.4.1.5. Связанные команды

Загрузка файла

Команда	**copy flash:**[*local-directory/*]*local-file* **ftp:** *//username:password@dest-address*[*/remote-directory*] */remote-file*
Описание параметров	*local-directory:* указывает каталог на локальном устройстве. Если он не указан, указывает на текущий каталог. local-file: указывает локальный файл для загрузки. username: указывает имя пользователя для доступа к FTP-серверу, состоящему из не более 32 байт и исключая такие разделители, как / : @ и пробел. Этот параметр является обязательным. password: указывает пароль для доступа к FTP-серверу, состоящий не более чем из 32 байт и исключая такие разделители, как / : @ и пробел. Этот параметр является обязательным. dest-address: указывает IP-адрес для FTP-сервера. remote-directory: указывает каталог на сервере. remote-file: переименовывает файл на сервере. **ПРИМЕЧАНИЕ:** на устройстве должен быть создан каталог, указанный в поле *local-directory*. Эта команда не создает каталог автоматически
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы загрузить файл с флеш-памяти локального устройства на FTP-сервер

Загрузка файла FTP

Команда	**copy ftp:***//username:password@dest-address*[*/remote-directory*]*/remote-file* **flash:**[*local-directory/*]*local-file*
Описание параметров	*username*: указывает имя пользователя для доступа к FTP-серверу, состоящему из не более 32 байт и исключая такие разделители, как / : @ и пробел. Этот параметр является обязательным. *password:* указывает пароль для доступа к FTP-серверу, состоящий не более чем из 32 байт и исключая такие разделители, как / : @ и пробел. Этот параметр является обязательным.

	dest-address: указывает IP-адрес для FTP-сервера. *remote-directory:* указывает каталог на сервере. *remote-file:* указывает файл для загрузки. *local-directory:* указывает каталог на локальном устройстве. Если он не указан, указывает на текущий каталог. *local-file:* переименовывает файл в локальной флеш-памяти. **ПРИМЕЧАНИЕ:** на устройстве должен быть создан каталог, указанный в поле *local-directory*. Эта команда не создает каталог автоматически
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы загрузить файл с FTP-сервера во флеш-память локального устройства

8.4.1.6. Пример конфигурации

Загрузка файла

Этапы конфигурации	Загрузите локальный файл **local-file** в домашний каталог **home** устройства в корневой каталог **root** FTP-сервера с именем пользователя **user**, паролем **pass** и IP-адресом **192.168.23.69** и именем файла **remote-file**
	QTECH# copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file
Проверка конфигурации	Проверьте, существует ли файл удаленного файла на FTP-сервере

Скачивание файла

Этапы конфигурации	Загрузите файл **remote-file** из корневого каталога **root** FTP-сервера с именем пользователя **user**, паролем **pass** и IP-адресом **192.168.23.69** в домашний каталог **home** устройства и сохраните файл как **local-file**
	QTECH# copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file
Проверка конфигурации	Проверьте, существует ли файл **remote-file** в домашнем каталоге **home** флеш-памяти

8.4.1.7. Типичные ошибки

- Форматы команд для загрузки и скачивания неверны.

- Неверное имя пользователя или пароль.

8.4.2. Настройка дополнительных функций

8.4.2.1. Результат конфигурации

Установите режимы подключения и передачи и настройте исходный IP-адрес клиента для загрузки и скачивания файлов.

8.4.2.2. Примечания

Если необходимо настроить клиент FTP на основе VRF, сначала укажите VRF.

8.4.2.3. Этапы конфигурации

Установка режима подключения в активное (Port)

- Опционально.
- Настройте режим подключения FTP.

Установите режим передачи в ASCII

- Опционально.
- Настройте режим передачи FTP.

Настройте исходный IP-адрес клиента FTP

- Опционально.
- Настройте исходный IP-адрес клиента FTP.

Восстановление настроек по умолчанию

- Опционально.
- Восстановите настройки клиента FTP по умолчанию.

8.4.2.4. Проверка конфигурации

Выполните команду **show run**, чтобы проверить результат.

8.4.2.5. Связанные команды

Установка режима подключения в активное (Port)

Команда	**ftp-client** [**vrf** *vrf-name*] **port**
Описание параметров	**vrf** *vrf-name*: указывает VRF
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы установить режим подключения на активный (PORT). По умолчанию используется пассивный режим подключения (PASV)

Настройте исходный IP-адрес клиента FTP

Команда	**ftp-client** [**vrf** *vrfname*] **source-address** {*ip-address* | *ipv6address*}
Описание параметров	**vrf** *vrf-name*: указывает VRF. *ip-address:* указывает IPv4-адрес локального интерфейса. *ipv6-address:* указывает IPv6-адрес локального интерфейса
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы настроить IP-адрес интерфейса клиента для подключения к серверу. По умолчанию для клиента не задан локальный IP-адрес. Вместо этого маршрут выбирает IP-адрес для клиента

Установите режим передачи в ASCII

Команда	**ftp-client** [**vrf** *vrf-name*] **ascii**
Описание параметров	**vrf** *vrf-name*: указывает VRF
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы установить режим передачи ASCII. По умолчанию используется двоичный режим передачи

Восстановление настроек по умолчанию

Команда	**default ftp-client** [**vrf** *vrf-name*]
Описание параметров	**vrf** *vrf-name*: указывает VRF
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы восстановить настройки по умолчанию, а именно, режим подключения, установленный на пассивный (PASV), режим передачи двоичного кода и IP-адрес источника удален

8.4.2.6. Пример конфигурации

Настройка дополнительных функций

Этапы конфигурации	• Установите режим подключения FTP к порту. • Установите режим передачи ASCII. • Установите IP-адрес источника на 192.168.23.167. • Установите режим подключения vrf 123 на порт. • Установите режим передачи vrf 123 в ASCII
	QTECH# configure terminal QTECH(config)# ftp-client ascii QTECH(config)# ftp-client port QTECH(config)# ftp-client source-address 192.168.23.167 QTECH(config)# ftp-client vrf 123 port QTECH(config)# ftp-client vrf 123 ascii QTECH(config)# end
Проверка конфигурации	Запустите команду **show run** на устройстве, чтобы проверить, действует ли конфигурация. QTECH# show run ! ftp-client ascii ftp-client port ftp-client vrf 123 port ftp-client vrf 123 ascii ftp-client source-address 192.168.23.167 !

8.4.2.7. Типичные ошибки

- Исходный IP-адрес не является локальным IP-адресом.
- Перед настройкой команды **ftp-client vrf** настройте команду **vrf**.

8.5. Контроль состояния

8.5.1. Отображение

Описание	Команда
Отображает конфигурацию FTP-клиента	**show run**

8.5.2. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Отладка FTP-клиента	**debug ftp-client**

9. НАСТРОЙКА ТУННЕЛЬНОГО ИНТЕРФЕЙСА

9.1. Обзор

Интерфейсы туннелей — это виртуальные интерфейсы, используемые для внедрения туннелирования. Туннельный интерфейс обеспечивает стандартный канал передачи, и вам не нужно указывать транспортный протокол или протокол полезной нагрузки. Каждый интерфейс туннеля представляет собой канал передачи.

Функция туннелирования включает следующие компоненты:

- Контроль нагрузки: используется для инкапсуляции данных, передаваемых в туннелях. Например, протоколы IPv4 и IPv6 работают как протоколы полезной нагрузки. Туннели с общей инкапсуляцией маршрутизации (GRE) могут передавать данные IPv4 или IPv6.
- Протокол передачи данных: используется для вторичной инкапсуляции и идентификации передаваемых данных. В туннелях, описанных в настоящем документе, используется только туннель GRE с протоколом передачи данных, то есть протоколом GRE. В других туннелях используются протоколы IPv4 и IPv6. Пакеты инкапсулируются с внешними заголовками IPv4 и IPv6.
- Протокол транспорта: используется для передачи данных, инкапсулированных во второй раз по протоколу передачи данных. Оборудование QTECH используют широко применяемые протоколы IPv4 и IPv6 в качестве транспортных протоколов.

Туннельный режим можно использовать для установления связи между двумя частными сетями, использующими один и тот же протокол, через гетерогенную общедоступную сеть.

Туннелирование применимо к следующим сценариям:

- Поскольку туннелирование поддерживает различные протоколы полезной нагрузки, оно позволяет осуществлять связь между локальными сетями, в которых используются протоколы, отличные от IP, через единую сеть (IP-сеть). Поскольку туннелирование работает на маршрутах, использующих транспортные протоколы (IP-протоколы), оно позволяет более широко применять протоколы с ограничением переходов.
- Туннелирование позволяет подключать отдельные подсети через единую сеть (IP-сеть).
- Туннелирование позволяет включить функцию виртуальной частной сети (VPN) в глобальных сетях (WAN).

Инкапсулированные данные передаются через туннели, что является сложным процессом. В некоторых случаях необходимо обратить внимание на следующие изменения:

- Поскольку туннель является логическим каналом, он, по-видимому, является одним переходом в маршрутизации. Однако фактически стоимость пути может быть более одного перехода. При использовании туннеля для передачи обратите внимание, что маршрут канала туннеля отличается от фактического маршрута.
- При настройке брандмауэра или списка контроля доступа (ACL) примите во внимание конфигурацию туннеля. Пропускная способность и максимальный размер передаваемого пакета (MTU), разрешенный протоколами полезной нагрузки, меньше теоретических значений.

9.1.1. Протоколы и стандарты

- RFC2784: общая инкапсуляция маршрута (GRE).

- RFC2890: расширения ключа и порядкового номера для GRE.
- RFC3056: подключение доменов IPv6 через облака IPv4.
- RFC3068: Anycast Prefix для ретрансляторных маршрутизаторов 6на4.
- RFC3964: вопросы безопасности для 6на4.
- RFC4023: инкапсуляция MPLS в инкапсуляции IP или общей маршрутизации (GRE).
- RFC4087: IP-туннель MIB.
- RFC4213: базовые механизмы перехода для хостов и маршрутизаторов IPv6.
- RFC4797: использование общей инкапсуляции маршрутизации (GRE) или IP-адреса в виртуальных частных IP-сетях BGP/MPLS IP (PE-PE).
- RFC5158: спецификация делегирования 6на4 обратного DNS.
- RFC5214: внутрисайтовая автоматическая адресация туннелей (ISATAP).
- RFC5332: многоадресная инкапсуляция MPLS.
- RFC5579: передача пакетов IPv4 по интерфейсам протокола автоматического туннелирования (ISATAP) на внутрисайтовой основе.
- RFC5845: параметр ключа общей инкапсуляции маршрутизации (GRE) для мобильного прозрачного (proxy) IPv6.
- RFC6245: расширение ключа общей инкапсуляции маршрутизации (GRE) для мобильного IPv4.
- RFC6343: рекомендации по развертыванию 6на4.
- RFC6372: управляемые провайдером туннели 6на4.
- Опции draft-zhou-dhc-gre-option-00 DHCPv4 и DHCPv6 для GRE.
- draft-templin-v6ops-isops-18 Руководство по эксплуатации развертывания IPv6 на узлах IPv4 с использованием ISATAP.

9.2. Применение

Применение	Описание
Доступ к сайтам IPv6 в сети кампуса	Доступ к сайтам IPv6 в кампусной сети
Подключение сети кампуса к магистральной сети IPv6	Соединяет сеть комплекса зданий с магистральной сетью IPv6

9.2.1. Доступ к сайтам IPv6 в сети кампуса

9.2.1.1. Сценарий

Серверы IPv6 развертываются в некоторых кампусных сетях, и ПК должны иметь доступ к серверам. Для реализации доступа можно использовать внутрисайтовый протокол автоматической адресации туннелей (ISATAP).

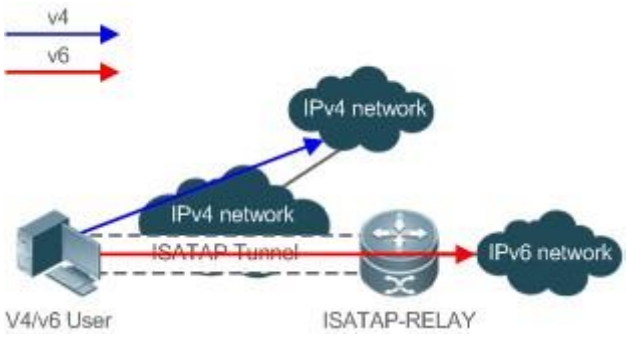


Рисунок 9-1.

ISATAP-RELAY поддерживает туннелирование. Пользователи в кампусной сети могут получать доступ к серверам IPv4 напрямую через сеть IPv4, но им требуется доступ к серверам IPv6 через туннель ISATAP.

9.2.1.2. Описание

- Пользователи IPv4 и IPv6 получают доступ к сети IPv4 с помощью адресов IPv4.
- Пользователи IPv4 и IPv6 получают доступ к сети IPv6 через туннель ISATAP.
- Туннель ISATAP устанавливается между ПК и маршрутизатором ISATAPRELAY.

9.3. Настройка

Настройка	Описание и команда	
Настройка туннельного интерфейса	(Обязательно) используется для создания туннелей	
	Interface tunnel	Создает туннельный интерфейс
	tunnel source	Настраивает локальный адрес туннеля
Настройка режима туннеля	(ОПЦИОНАЛЬНО) используется для настройки режима туннеля	
	tunnel mode	Настраивает режим инкапсуляции туннеля
Настройка локального адреса	(Необязательно) используется для настройки локального адреса туннеля	
	tunnel source	Настраивает адрес туннеля
Настройка адреса одноранговой сети	(Необязательно) используется для настройки одноранговой адреса туннеля	
	tunnel destination	Настройка адреса одноранговой сети туннеля

Настройка	Описание и команда	
Настройка TOS туннеля	(ОПЦИОНАЛЬНО) используется для настройки типа обслуживания (TOS) туннеля	
	tunnel tos	Настройка TOS-туннеля
Настройка TTL туннеля	(ОПЦИОНАЛЬНО) используется для настройки времени жизни (TTL) туннеля	
	tunnel ttl	Настройка TTL-туннеля

9.3.1. Настройка туннельного интерфейса

9.3.1.1. Результат конфигурации

Создайте туннельный интерфейс.

9.3.1.2. Этапы конфигурации

Создание туннельного интерфейса

- Выполните команду **interface tunnel** *number* в режиме глобальной конфигурации для создания интерфейса туннеля.
- Служба туннелирования доступна только после создания интерфейса туннеля.

9.3.1.3. Проверка конфигурации

Выполните команду **show interface tunnel** *number*, чтобы проверить, успешно ли создан туннельный интерфейс.

9.3.1.4. Связанные команды

Настройка интерфейса туннеля

Команда	**interface tunnel** *number*
Описание параметров	*number*: указывает номер интерфейса туннеля
Режим конфигурации	Режим глобальной конфигурации

Проверка конфигурации туннеля

Команда	**show interface tunnel** *number*
Описание параметров	*number*: указывает номер интерфейса туннеля
Режим конфигурации	Режим глобальной конфигурации

9.3.1.5. Пример конфигурации

Создание туннельного интерфейса

Этапы конфигурации	Создайте туннельный интерфейс
	QTECH# configure terminal QTECH(config)# interface tunnel 1 QTECH(config-if-Tunnel 1)# end
Проверка конфигурации	Проверьте конфигурацию интерфейса туннеля
	QTECH# show interface tunnel 1 …… Tunnel attributes: …… Tunnel protocol/transport is gre ip

9.3.1.6. Типичные ошибки

- Невозможно создать туннельный интерфейс из-за нехватки памяти.
- Невозможно создать туннельный интерфейс из-за нехватки аппаратных ресурсов.

9.3.2. Настройка режима туннеля

9.3.2.1. Результат конфигурации

Настройте режим инкапсуляции туннеля в режиме конфигурации интерфейса туннеля, если необходимо использовать туннель в режиме инкапсуляции, не установленном по умолчанию.

9.3.2.2. Этапы конфигурации

Настройка режима туннеля

- Опционально.
- Режим инкапсуляции коммутаторов по умолчанию — туннельный режим ipv6ip.

- Чтобы изменить режим инкапсуляции по умолчанию, выполните команду **tunnel mode** в режиме конфигурации интерфейса туннеля.

9.3.2.3. Проверка конфигурации

Выполните команду **show interface tunnel** *number*, чтобы проверить, настроен ли режим инкапсуляции туннеля.

9.3.2.4. Связанные команды

Настройка режима туннеля

Команда	**tunnel mode** { **gre** {**ip | ipv6**} | **ipv6 | ipip | ipv6ip [6to4 | isatap]** }
Описание параметров	Каждый режим соответствует разным форматам инкапсуляции пакетов, отправленных интерфейсом туннеля. **gre ip** указывает, что пакет инкапсулирован с заголовком GRE и заголовком IPv4 последовательно, а затем передается по новой сети IPv4. **gre ipv6** указывает, что пакет инкапсулирован с заголовком GRE и заголовком IPv6 последовательно, а затем передается по новой сети IPv6. **ipv6** указывает, что пакет, отправленный через туннельный интерфейс, инкапсулируется с заголовком IPv6, а затем передается по новой сети IPv6. **ipip** указывает, что туннельный интерфейс передает только пакеты IPv4, а пакет, отправленный через туннельный интерфейс, инкапсулируется с заголовком IPv4, а затем передается по новой сети IPv4. **Ipv6ip** указывает, что туннельный интерфейс передает только пакеты IPv6, а пакет, отправленный через туннельный интерфейс, инкапсулируется с заголовком IPv4, а затем передается по новой сети IPv4. Предшествующие туннели представляют собой туннели с ручным управлением, а туннели с протоколом IPv6IP, 6to4 и ISATAP являются автоматическими. Во время инкапсуляции пакетов адрес IPv4 назначения сопоставляется с адресом IPv6 назначения
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	На обоих концах туннеля должен быть настроен один и тот же режим инкапсуляции. В противном случае туннель не сможет работать

9.3.2.5. Пример конфигурации

Настройка IPv4 в режиме инкапсуляции IPv4

Этапы конфигурации	Настройте режим инкапсуляции IPv4 через IPv4 на интерфейсе туннеля
	QTECH# configure terminal QTECH(config)# interface tunnel 1 QTECH(config-if-Tunnel 1)# tunnel mode ipip QTECH(config)# end
Проверка конфигурации	Проверьте конфигурацию интерфейса туннеля
	QTECH# show interface tunnel 1 …… Tunnel attributes: …… Tunnel protocol/transport is ipip

9.3.2.6. Типичные ошибки

Туннель 6to4 или ISATAP настроен для виртуального экземпляра маршрутизации и пересылки (VRF), который уже настроен с туннелем 6to4/ISATAP.

9.3.3. Настройка локального адреса

9.3.3.1. Результат конфигурации

Настройте локальный адрес туннеля.

9.3.3.2. Примечания

- Локальный адрес туннеля должен совпадать с транспортным протоколом, используемым туннелем. В противном случае интерфейс туннеля не будет работать (будет отключен).
- Если локальный адрес указан косвенно путем настройки другого интерфейса, локальный адрес является основным адресом IPv4 или первым глобальным общедоступным адресом IPv6.

9.3.3.3. Этапы конфигурации

Настройка локального адреса

- Обязательно.
- Выполните команду **tunnel source** в режиме конфигурации интерфейса туннеля, чтобы указать локальный адрес туннеля.

9.3.3.4. Проверка конфигурации

Выполните команду **show interface tunnel** *number*, чтобы отобразить локальный адрес туннеля.

9.3.3.5. Связанные команды

Настройка локального адреса

Команда	**tunnel source** { *ip-address* | *interface-name interface-number* }
Описание параметров	**ip-address**: указывает адрес IPv4 или IPv6. *Interface-name interface-number*: указывает на интерфейс уровня 3
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Если адрес IPv4 или IPv6 указан напрямую, необходимо настроить адрес устройства

9.3.3.6. Пример конфигурации

Настройка локального адреса

Этапы конфигурации	Настройте локальный адрес туннеля как 1.1.1.1
	QTECH# configure terminal QTECH(config)# interface tunnel 1 QTECH(config-if-Tunnel 1)# tunnel mode ipip QTECH(config-if-Tunnel 1)# tunnel source 1.1.1.1
Проверка конфигурации	Проверьте конфигурацию интерфейса туннеля
	QTECH# show interface tunnel 1 …… Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class not set, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipip Tunnel transport VPN is no set ……

9.3.4. Настройка адреса одноранговой сети

9.3.4.1. Результат конфигурации

Туннель в ручном режиме можно использовать (интерфейс туннеля работает) только после настройки адреса одноранговой сети.

9.3.4.2. Примечания

Адреса одноранговых узлов не могут быть настроены для автоматических туннелей.

9.3.4.3. Этапы конфигурации

Настройка адреса одноранговой сети

- Адреса одноранговых узлов должны быть настроены для всех туннелей, кроме туннелей 6to4 и ISATAP.
- Выполните команду **tunnel destination** в режиме конфигурации интерфейса, чтобы настроить адрес одноранговой сети туннеля.

9.3.4.4. Проверка конфигурации

Выполните команду **show interface tunnel**, чтобы проверить, настроен ли адрес назначения.

9.3.4.5. Связанные команды

Настройка адреса одноранговой сети

Команда	**tunnel destination** { *ip-address* }
Описание параметров	***ip-address***: указывает адрес IPv4 или IPv6
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	Необходимо настроить одноранговый адрес туннеля вручную. Тип набора протоколов настроенного адреса однорангового узла должен соответствовать протоколу транспорта, используемому туннелем. Если они не совпадают, интерфейс туннеля будет отключен (down)

9.3.4.6. Пример конфигурации

Настройка адреса одноранговой сети

Этапы конфигурации	Настройте одноранговый адрес туннеля как 2.2.2.2
	QTECH# configure terminal QTECH(config)# interface tunnel 1 QTECH(config-if-Tunnel 1)# tunnel mode ipip

	QTECH(config-if-Tunnel 1)# tunnel destination 2.2.2.2
Проверка конфигурации	Проверьте конфигурацию интерфейса туннеля
	QTECH# show interface tunnel 1 …… Tunnel attributes: Tunnel source: UNKNOWN, destination 2.2.2.2, unrouteable Tunnel TOS/Traffic Class not set, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipip ……

9.3.4.7. Типичные ошибки

- Адрес одноранговой сети настроен для автоматического туннеля.
- Адрес одноранговой сети, настроенный для туннеля, совпадает с адресом другого туннеля.

9.3.5. Настройка TOS туннеля

9.3.5.1. Результат конфигурации

Укажите поле TOS или Traffic Class в заголовке транспортного протокола.

9.3.5.2. Примечания

Если поле TOS или Traffic Class в заголовке транспортного протокола не указано, поле TOS или Traffic Class протокола копируется в заголовок.

9.3.5.3. Этапы конфигурации

Настройка TOS туннеля

- Опционально.
- Чтобы изменить приоритет данных туннеля в сети, выполните команду **tunnel tos** в режиме конфигурации интерфейса.

9.3.5.4. Проверка конфигурации

Запустите команду **show interface tunnel**, чтобы проверить, настроена ли TOS.

9.3.5.5. Связанные команды

Настройка TOS туннеля

Команда	**tunnel tos** *number*
Описание параметров	***number***: указывает TOS туннеля
Режим конфигурации	Режим конфигурации интерфейса
Встроенная подсказка	По умолчанию, если протокол IPv4 используется для внутренней и внешней инкапсуляции в туннеле, TOS-байты во внутреннем заголовке IPv4 копируются во внешний заголовок IPv4. Если протокол IPv6 используется для внутренней и внешней инкапсуляции канала, то бит класса трафика 8 во внутреннем заголовке IPv6 копируется во внешний заголовок IPv6. В других случаях поле TOS во внешнем заголовке IPv4 и поле Traffic Class в заголовке IPv6 имеют значение 0

9.3.5.6. Пример конфигурации

Настройка TOS туннеля

Этапы конфигурации	Настройка TOS туннеля
	QTECH# configure terminal QTECH(config)# interface tunnel 1 QTECH(config-if-Tunnel 1)# tunnel mode ipip QTECH(config-if-Tunnel 1)# tunnel tos 2
Проверка конфигурации	Проверьте конфигурацию интерфейса туннеля
	QTECH# show interface tunnel 1 …… Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipip Tunnel transport VPN is VPN1 ……

9.3.6. Настройка TTL туннеля

9.3.6.1. Результат конфигурации

Укажите предел кол-ва переходов или TTL для заголовков протокола инкапсуляции туннеля.

9.3.6.2. Этапы конфигурации

Настройка TTL туннеля

- Опционально.
- По умолчанию значение TTL равно 255, что является максимальным значением.
- Чтобы уменьшить ограничение длины канала туннеля, выполните команду TTL туннеля.

9.3.6.3. Проверка конфигурации

Запустите команду **show interface tunnel**, чтобы проверить, настроен ли TTL.

9.3.6.4. Связанные команды

Настройка TTL туннеля

Команда	**tunnel ttl** *hop-limit*
Описание параметров	*hop-limit*: указывает предел переходов для туннеля
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Ограничение переходов указывает максимальное количество маршрутизаторов, через которые может проходить пакет. Значение по умолчанию — 255. Эта команда используется для уменьшения ограничения количества переходов

9.3.6.5. Пример конфигурации

Настройка TTL туннеля

Этапы конфигурации	Настройка TTL туннеля
	QTECH# configure terminal QTECH(config)# interface tunnel 1 QTECH(config-if-Tunnel 1)# tunnel mode ipip QTECH(config-if-Tunnel 1)# tunnel ttl 3
Проверка конфигурации	Проверьте конфигурацию интерфейса туннеля

	QTECH# show interface tunnel 1 …… Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipip Tunnel transport VPN is VPN1

9.4. Контроль состояния

9.4.1. Отображение

Описание	Команда
Отображает информацию об интерфейсе туннеля	**show interface tunnel** *number*

9.4.2. Отладка

Системные ресурсы заняты при выводе отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Включает отладку интерфейса туннеля	**debug tunnel**

10. ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ СЕТЕВЫХ СОЕДИНЕНИЙ

10.1. Обзор

Средства тестирования сетей связи можно использовать для проверки подключения сети, а также для анализа и обнаружения неисправностей сети. Средства тестирования сетевых коммуникаций включают в себя инструменты проверки пакетов в Интернете (PING) и Traceroute. Ping используется для проверки соединения и задержки сети. Большая задержка указывает на более низкую скорость сети. Функция traceroute помогает узнать топологию физических и логических каналов и скорость передачи данных. На сетевом устройстве можно выполнить команды **ping** и **traceroute**, чтобы использовать два инструмента соответственно.

10.1.1. Протоколы и стандарты

- RFC792: протокол сообщений управления Интернетом.
- RFC4443: протокол ICMPv6 для протокола Интернета версии 6 (IPv6).

10.2. Применение

Применение	Описание
Тестирование связности End-to-End	Сетевое устройство и узел назначения подключены к IP-сети и настроены с IP-адресами
Тест маршрута хоста	Сетевое устройство и узел назначения подключены к IP-сети и настроены с IP-адресами

10.2.1. Тестирование связности End-to-End

10.2.1.1. Сценарий

Как показано на Рисунке 10-1, сетевое устройство A и целевой хост B подключены к IP-сети.

Если сетевое устройство и целевой хост подключены к IP-сети, целью теста сквозного подключения является проверка возможности передачи IP-пакетов между двумя концами. Целевой хост может быть самим сетевым устройством. В этом случае тест подключения предназначен для проверки сетевого интерфейса и конфигурации TCP/IP на устройстве.

Рисунок 10-1.

10.2.1.2. Описание

Выполните функцию ping на сетевом устройстве.

10.2.2. Тест маршрута хоста

10.2.2.1. Сценарий

Как показано на Рисунке 10-2, сетевое устройство A и целевой хост B подключены к IP-сети.

Если и сетевое устройство, и целевой хост подключены к IP-сети, тест маршрута хоста направлен на проверку шлюзов (или маршрутизаторов), через которые проходят IP-пакеты между двумя концами соединения. Как правило, целевой хост находится не в том же сегменте IP-сети, что и сетевое устройство.

Рисунок 10-2.

10.2.2.2. Описание

Выполните функцию трассировки на сетевом устройстве.

10.3. Ключевые особенности

10.3.1. Обзор

Функция	Описание
Ping-тест	Проверьте, доступен ли указанный адрес IPv4 или IPv6, и отобразите соответствующую информацию
Проверка трассировки	Отобразите шлюзы, через которые проходят пакеты IPv4 или IPv6 при передаче от источника к адресату

10.3.2. Ping-тест

10.3.2.1. Принцип работы

Инструмент ping отправляет сообщение запроса протокола ICMP на узел назначения, чтобы запросить сообщение ICMP Echo Reply. Таким образом, инструмент ping определяет задержку и соединение между двумя сетевыми устройствами.

10.3.2.2. Связанная конфигурация

Выполните команду **ping**.

10.3.3. Проверка трассировки

10.3.3.1. Принцип работы

Инструмент traceroute использует поле Time to Live (TTL) в заголовках ICMP- и IP-сообщений для теста. Сначала средство traceroute на сетевом устройстве отправляет ICMP-сообщение с TTL 1 на узел назначения. После получения сообщения первый маршрутизатор на пути уменьшает TTL на 1. По мере того, как TTL становится 0, маршрутизатор сбрасывает пакеты и возвращает сообщение ICMP Time exceeded на сетевое устройство. После получения этого сообщения средство traceroute обнаруживает,

что этот маршрутизатор существует на данном пути, а затем отправляет пакет запроса ICMP с TTL 2 на узел назначения для обнаружения второго маршрутизатора. Каждый раз, когда инструмент traceroute увеличивает TTL в сообщении запроса ICMP на 1 обнаруживается еще один маршрутизатор. Этот процесс повторяется до тех пор, пока пакет данных не достигнет узла назначения. После того как пакет достигнет узла назначения, узел возвращает сообщение ICMP Echo вместо сообщения ICMP Time Exceeded на сетевое устройство. Затем инструмент traceroute завершает тест и отображает путь от сетевого устройства к узлу назначения.

10.3.3.2. Связанная конфигурация

Выполните команду **traceroute**.

10.4. Настройка

Настройка	Описание и команда	
Ping-тест	(Необязательно) используется для проверки доступности адреса IPv4 или IPv6	
	ping	Выполняет функцию Ping
Проверка трассировки	(Необязательно) используется для отображения шлюзов, через которые проходят пакеты IPv4 или IPv6 при передаче из источника в назначение	
	traceroute	Выполняет функцию traceroute

10.4.1. Ping-тест

10.4.1.1. Результат конфигурации

После выполнения ping-теста на сетевом устройстве можно узнать, подключено ли сетевое устройство к узлу назначения и можно ли передавать пакеты между сетевым устройством и узлом назначения.

10.4.1.2. Примечания

На сетевом устройстве должен быть настроен IP-адрес.

10.4.1.3. Этапы конфигурации

- Чтобы проверить, доступен ли адрес IPv4, используйте команду **ping IPv4**.
- Чтобы проверить, доступен ли адрес IPv6, используйте команду **ping IPv6**.

10.4.1.4. Проверка конфигурации

Выполните команду **ping**, чтобы отобразить соответствующую информацию в окне интерфейса командной строки (CLI).

10.4.1.5. Связанные команды

Ping IPv4

Команда	**ping** [**oob** | **vrf** *vrf-name* | **ip**] [*address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond]]
Описание параметров	**oob**: указывает использование MGMT-интерфейса как источника. Этот параметр необходимо настроить, если порт MGMT указан в качестве исходного порта. *vrf-name*: указывает имя маршрутизации и пересылки VPN (VRF). *address*: указывает адрес IPv4 назначения или имя домена. *mgmt-name:* указывает порт MGMT в режиме OOB. *length*: указывает длину пакета данных. Диапазон значений от 36 до 18 024. Длина по умолчанию — 100. *times*: указывает количество запросов. Диапазон значений от 1 до 4 294 967 295 *seconds*: указывает время ожидания. Значение варьируется от 1 до 10 секунд. *data*: указывает данные в пакете. Данные - это строка размером от 1 до 255 байт. По умолчанию строка имеет значение "abcd". *source*: указывает исходный адрес IPv4 или порт-источник пакета. Адрес интерфейса обратной связи, например, 127.0.0.1, не может использоваться в качестве исходного адреса. **df-bit**: настройка бита DF IP-адреса. Если для бита DF установлено значение 1, пакет не фрагментирован. По умолчанию бит DF имеет значение 0. **validate**: настройка проверки ответного пакета. **detail**: настройка отображения сообщения Echo Reply (эхо-ответ) подробно. По умолчанию используется только восклицательный знак (!) и точка (.). millisecond: указывает интервал отправки пакета ping. Значение варьируется от 10 мс до 300 000 мс. Интервал по умолчанию составляет 100 мс
Режим конфигурации	В режиме User EXEC можно выполнить только базовую функцию ping. В режиме Privileged EXEC можно выполнить расширенную функцию ping. В других режимах настройки можно выполнить команду **do** для выполнения расширенной функции ping. Для получения дополнительной информации о конфигурации см. описание команды **do**

Использование конфигурации	При выполнении функции ping отображается информация об ответе (если таковой имеется), а затем выводится соответствующая статистика. С помощью функции расширенного ping можно указать количество, длину и время ожидания пакетов для отправки. Как и в базовой функции ping, будет выводиться соответствующая статистика. Чтобы использовать имя домена, необходимо сначала настроить сервер доменных имен (DNS). Подробнее о настройке см. в разделе Настройка DNS

Ping IPv6

Команда	**ping** [**vrf** *vrf-name* | [**oob**] **ipv6**] [*address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**] [**interval** millisecond] [**out-interface** interface]]
Описание параметров	**oob**: указывает использование MGMT-интерфейса как источника. Этот параметр необходимо настроить, если порт MGMT указан в качестве исходного порта. *vrf-name*: указывает имя VRF. *address*: указывает адрес IPv6 назначения или имя домена. *mgmt-name:* указывает порт MGMT в режиме OOB. *length*: указывает длину пакета данных. Диапазон значений от 16 до 18 024. Длина по умолчанию — 100. *times*: указывает количество запросов. Диапазон значений от 1 до 4 294 967 295. *seconds*: указывает время ожидания. Значение варьируется от 1 до 10 с. *data*: указывает данные в пакете. Данные - это строка размером от 1 до 255 байт. *source*: указывает исходный адрес IPv6 или порт-источник пакета. Адрес интерфейса loopback, например::1, не может использоваться в качестве исходного адреса. **detail**: настройка отображения сообщения Echo Reply (эхоответ) подробно. По умолчанию используется только восклицательный знак (!) и точка (.). millisecond: указывает интервал отправки пакета ping. Значение варьируется от 10 мс до 300 000 мс. Интервал по умолчанию составляет 100 мс

Режим конфигурации	В режиме User EXEC можно выполнить только базовую функцию ping IPv6. В режиме Privileged EXEC можно выполнить расширенную функцию ping IPv6. В других режимах настройки можно выполнить команду **do** для выполнения расширенной функции ping. Для получения дополнительной информации о конфигурации см. описание команды **do**
Использование конфигурации	При выполнении функции ping IPv6 отобразится информация об ответе (если таковой имеется), а затем будет выведена соответствующая статистика. С помощью IPv6 функции расширенного ping можно указать количество, длину и время ожидания пакетов для отправки. Как и в базовой IPv6 функции ping, будет выводиться соответствующая статистика. Чтобы использовать имя домена, необходимо сначала настроить DNS. Подробнее о настройке см. в разделе 6 Настройка DNS

10.4.1.6. Пример конфигурации

Выполнение базовой функции Ping

Этапы конфигурации	В привилегированном режиме EXEC выполните команду **ping 192.168.21.26**
	Common ping command: QTECH# ping 192.168.21.26 Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms Detailed ping command: QTECH#ping 192.168.21.26 detail Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: < press Ctrl+C to break > Reply from 192.168.21.26: bytes=100 time=4ms TTL=64 Reply from 192.168.21.26: bytes=100 time=3ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Проверка конфигурации	Отправьте пять пакетов размером 100 байт на указанный IP-адрес, и информация об ответе будет отображаться в указанное время (2 с по умолчанию). Далее выводится статистика

Выполнение функции расширенного Ping

Этапы конфигурации	В привилегированном режиме EXEC выполните команду **ping 192.168.21.26**. Кроме того, укажите длину, количество и время ожидания пакетов

	Common ping command: QTECH# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3 Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds: < press Ctrl+C to break > !! !! Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms Detailed ping command: ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds: < press Ctrl+C to break > Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms

Проверка конфигурации	Отправьте двадцать 1500-байтовых пакетов по указанному IP-адресу, и информация об ответе (если таковой имеется) будет отображаться в указанное время (по умолчанию 3 с). Далее выводится статистика

Выполнение функции Common Ping IPv6

Этапы конфигурации	В привилегированном режиме EXEC выполните команду **ping ipv6 2001::1**
	Common ping command: QTECH# ping ipv6 2001::1 Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms Detailed ping command: QTECH#ping 2001::1 detail Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Проверка конфигурации	Отправьте пять пакетов размером 100 байт на указанный IP-адрес, и информация об ответе будет отображаться в указанное время (2 с по умолчанию). Далее выводится статистика

Выполнение функции расширенного Ping IPv6

Этапы конфигурации	В привилегированном режиме EXEC выполните команду **ping ipv6 2001::5**. Кроме того, укажите длину, количество и время ожидания пакетов
	Common ping command: QTECH# ping ipv6 2001::5 length 1500 ntimes 100 data ffff source 2001::9 timeout 3 Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds: < press Ctrl+C to break > !! !! Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms Detailed ping command: QTECH#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3 Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds: < press Ctrl+C to break > Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms
Проверка конфигурации	Отправьте сто 1500-байтовых пакетов по указанному адресу IPv6, и информация об ответе (если таковой имеется) будет отображаться в указанное время (по умолчанию 3 с). Далее выводится статистика

10.4.2. Проверка трассировки

10.4.2.1. Результат конфигурации

После выполнения проверки трассировки на сетевом устройстве можно узнать о топологии маршрутизации между сетевым устройством и узлом назначения, а также о шлюзах, через которые пакеты отправляются с сетевого устройства на узел назначения.

10.4.2.2. Примечания

Сетевое устройство должно быть настроено на IP-адрес.

10.4.2.3. Этапы конфигурации

- Чтобы отследить маршрут, по которому будет следовать пакет IPv4 на узел назначения, выполните команду **traceroute IPv4**.
- Чтобы отследить маршрут, по которому будет следовать пакет IPv6 на узел назначения, выполните команду **traceroute IPv6**.

10.4.2.4. Проверка конфигурации

Выполните команду **traceroute**, чтобы отобразить соответствующую информацию в окне интерфейса командной строки.

10.4.2.5. Связанные команды

Traceroute IPv4

Команда	**traceroute** [**oob** | **vrf** *vrf-name* | **ip**] [*adress* [**via** *mgmt-name*] [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]
Описание параметров	**oob**: указывает использование MGMT-интерфейса как источника. Этот параметр необходимо настроить, если порт MGMT указан в качестве исходного порта. *vrf-name*: указывает имя VRF. *address*: указывает адрес IPv4 назначения или имя домена. *mgmt-name:* указывает порт MGMT в режиме OOB. *number*: указывает количество запросов. Диапазон значений от 1 до 255. *source*: указывает исходный адрес IPv4 или порт-источник пакета. Адрес интерфейса обратной связи, например, 127.0.0.1, не может использоваться в качестве исходного адреса. *seconds*: указывает время ожидания. Значение варьируется от 1 до 10 с. *minimum maximum*: указывает минимальное и максимальное значения TTL. Диапазон значений от 1 до 255

Режим конфигурации	В пользовательском EXEC-режиме можно выполнить только базовую функцию трассировки. В привилегированный EXEC-режиме можно выполнить расширенную функцию traceroute
Использование конфигурации	Команда **traceroute** используется для проверки сетевого подключения и точного определения неисправности при возникновении неисправности. Чтобы использовать имя домена, необходимо сначала настроить DNS. Подробнее о настройке см. в разделе 6 *Настройка DNS*

Traceroute IPv6

Команда	**traceroute** [**vrf** *vrf-name* | [**oob**] **ipv6**] [*address* [**via** *mgmtname*] [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*]
Описание параметров	**oob**: указывает локальное управление. Этот параметр необходимо настроить, если порт MGMT указан как порт источника. *vrf-name*: указывает имя VRF. *address*: указывает адрес IPv6 назначения или имя домена. *mgmt-name:* указывает порт MGMT в режиме OOB. *number*: указывает количество запросов. Диапазон значений от 1 до 255. *seconds*: указывает время ожидания. Значение варьируется от 1 до 10 с. *minimum maximum*: указывает минимальное и максимальное значения TTL. Диапазон значений от 1 до 255
Режим конфигурации	В режиме User EXEC можно выполнить только базовую функцию traceroute IPv6. В привилегированном режиме EXEC можно выполнить расширенную функцию traceroute IPv6
Использование конфигурации	Команда traceroute IPv6 используется для проверки сетевого подключения и точного определения места неисправности при возникновении неисправности. Чтобы использовать имя домена, необходимо сначала настроить DNS. Подробнее о настройке см. в разделе 6 *Настройка DNS*

10.4.2.6. Пример конфигурации

Выполнение функции Traceroute

Этапы конфигурации	В привилегированном режиме EXEC выполните команду **traceroute 5.134.219.3**
	QTECH#traceroute 5.134.219.3 < press Ctrl+C to break > Tracing the route to 202.108.37.42 1 192.168.12.1 0 msec 0 msec 0 msec 2 192.168.9.2 0 msec 4 msec 4 msec 3 192.168.110.1 16 msec 12 msec 16 msec 4 * * * 5 5.134.219.3 12 msec 28 msec 12 msec
	Предыдущий результат теста показывает, что сетевое устройство получает доступ к хосту 5.134.219.3, передавая пакеты через шлюзы 1–4. Кроме того, отображается время, необходимое для доступа к каждому шлюзу, а шлюз 4 неисправен

Выполнение функции Traceroute IPv6

Этапы конфигурации	В привилегированном режиме EXEC выполните команду **traceroute ipv6 3004::1**
	QTECH# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 3004::1 4 msec 28 msec 12 msec
	Предыдущий результат теста показывает, что сетевое устройство получает доступ к хосту 3004:1, передавая пакеты через шлюзы 1–4. Кроме того, отображается время, необходимое для доступа к каждому шлюзу

11. НАСТРОЙКА TCP

11.1. Обзор

Протокол управления передачей данных (TCP) — это протокол транспортного уровня, обеспечивающий надежные службы, ориентированные на подключение и IP, для уровня приложений.

Потоки межсетевых данных в 8-битных байтах передаются с уровня приложения на уровень TCP, а затем фрагментируются на сегменты пакетов надлежащей длины через TCP. Максимальный размер сегмента (MSS) обычно ограничивается максимальным размером передаваемого блока (MTU) на уровне канала данных. После этого пакеты отправляются на уровень IP, а затем на уровень TCP получателя по сети.

Чтобы предотвратить потерю пакетов, каждый байт идентифицируется по порядковым номерам через TCP, что обеспечивает получение пакетов, предназначенных для однорангового узла. После получения пакета получатель отправляет ответный пакет TCP ACK. Если отправитель не получает ACK-пакеты в течение разумного времени RRT, соответствующие пакеты (предположительно потерянные) будут переданы повторно.

- Протокол TCP использует функцию контрольной суммы для проверки целостности данных. Кроме того, для проверки данных можно использовать аутентификацию на основе MD5.
- Для обеспечения надежности используются механизм обратной передачи по таймауту и механизм обратной связи.
- Протокол скользящего окна используется для управления потоками. Как указано в Протоколе, неидентифицированные группы в окне должны быть переданы повторно.

11.1.1. Протоколы и стандарты

- RFC 793: протокол управления передачей.
- RFC 1122: требования к интернет-хостам — уровни связи.
- RFC 1191: обнаружение MTU пути.
- RFC 1213: управляемая база данных для сетевого администрирования на основе TCP/IP: MIB-II.
- RFC 2385: защита сеансов BGP с помощью опции подписи TCP MD5.
- RFC 4022: база управляющей информации для протокола управления передачей (TCP).

11.2. Применение

Применение	Описание
Оптимизация производительности TCP	Чтобы избежать фрагментации пакетов TCP на канале с небольшим MTU, включено обнаружение MTU пути (PMTUD)
Обнаружение исключения соединения TCP	TCP проверяет, работает ли одноранговый узел нормально

11.2.1. Оптимизация производительности TCP

11.2.1.1. Сценарий

Например, соединение TCP устанавливается между A и D, как показано на следующем Рисунке. MTU канала между A и B составляет 1500 байт, 1300 байт между B и C, и 1500 байт между C и D. Для оптимизации производительности передачи TCP следует избегать фрагментации пакетов между B и C.

Рисунок 11-1.

A, B, C и D являются маршрутизаторами.

11.2.1.2. Описание

Включите PMTUD на A и D.

11.2.2. Обнаружение исключения соединения TCP

11.2.2.1. Сценарий

Например, на следующем Рисунке пользователь входит в систему через telnet, но работает неправильно, как показано на следующем Рисунке. В случае тайм-аута повторной передачи TCP соединение пользователя TCP остается в течение длительного времени. Таким образом, TCP keepalive может быть использован для быстрого обнаружения исключения соединения TCP.

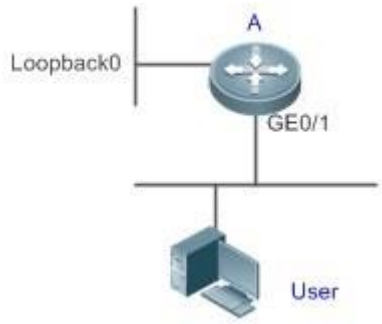


Рисунок 11-2.

A — это маршрутизатор.

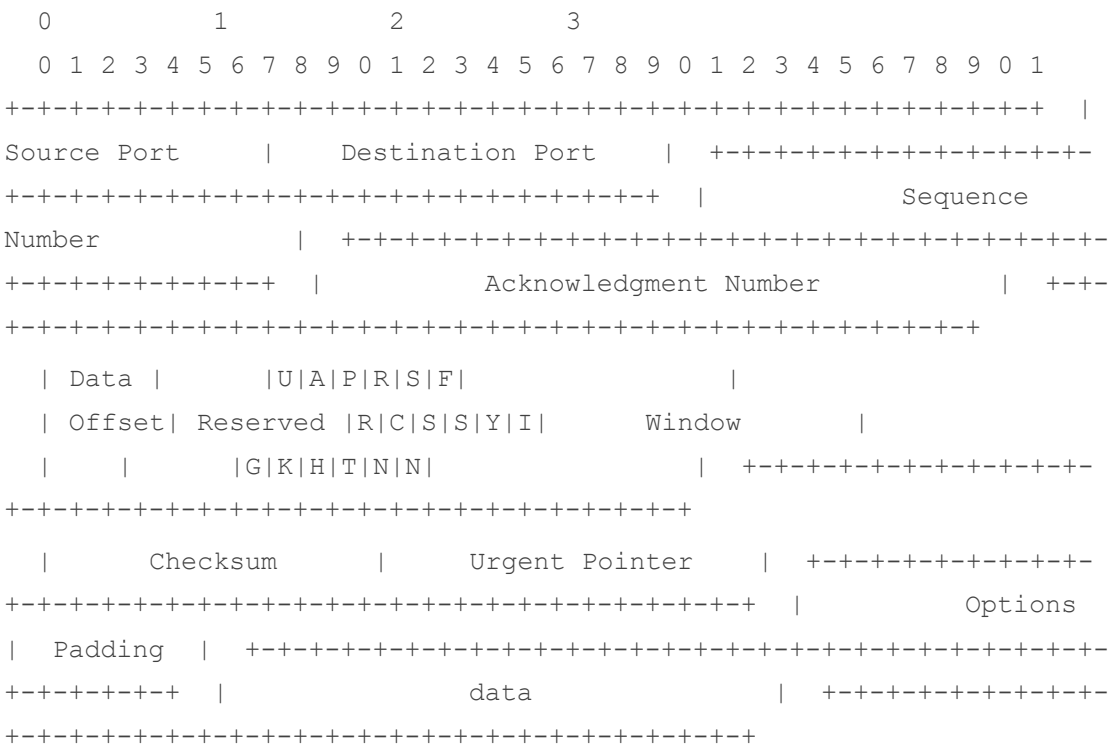
11.2.2.2. Описание

Включите поддержку TCP keepalive на A.

11.3. Ключевые особенности

11.3.1. Базовые концепции

Формат заголовка TCP



- **Source Port (Исходный порт)** — это 16-разрядный номер исходного порта.
- **Destination Port (Порт назначения)** — это 16-разрядный номер порта назначения.
- **Sequence Number (Порядковый номер)** — это 32-битный порядковый номер.
- **Acknowledgment Number (Номер подтверждения)** — это 32-битный номер, который определяет следующий порядковый номер, который должен получить получатель.
- **Data Offset** (**Смещение данных)** — это 4-разрядное число, указывающее общее количество байтов в заголовке TCP (опция включена), разделенное на 4.
- Бит флага — 6 бит. URG: поле срочного указателя является значимым; ACK: поле подтверждения является значимым; PSH: указывает на функцию push; RST: сбрасывает TCP-соединение; SYN: синхронизирует порядковый номер (устанавливает TCP-соединение); FIN: больше нет данных от отправителя (закрывает TCP-соединение).
- 16-битное значение окна используется для управления потоками. В нем указывается объем данных, которые могут передаваться из одноранговой узла между пакетами ACK.
- **Checksum (Контрольная сумма)** — это 16-разрядная контрольная сумма.
- **Urgent Pointer (Указатель срочных данных)** имеет 16-разрядную версию и показывает конец срочных данных, чтобы можно было продолжить прерванные потоки данных. При установке бита URG данные получают приоритет над другими потоками данных.

Трехсторонняя технология TCP Handshake

- Процесс трехстороннего квитирования TCP выполняется следующим образом:

1. Клиент отправляет на сервер пакет SYN.
2. Сервер получает пакет SYN и отвечает пакетом SYN ACK.
3. Клиент получает пакет SYN от сервера и отвечает пакетом ACK.

- После трехстороннего квитирования клиент и сервер успешно подключены и готовы к передаче данных.

11.3.2. Обзор

Функция	Описание
Настройка тайм-аута SYN	Настройка тайм-аута ожидания ответного пакета после отправки пакета SYN или SYN ACK
Настройка размера окна	Настройка размера окна
Настройка сброса отправки пакетов	Настройка отправки пакетов сброса TCP после получения сообщений порта вне доступа
Настройка MSS	Настройте MSS для подключения TCP
Обнаружение MTU пути	Найдите наименьший MTU на пути передачи TCP и отрегулируйте размер пакетов TCP на основе этого MTU, чтобы избежать фрагментации
TCP Keepalive	Проверьте, работает ли одноранговый узел нормально

11.3.3. Настройка тайм-аута SYN

11.3.3.1. Принцип работы

Соединение TCP устанавливается после трехстороннего квитирования: Отправитель отправляет пакет SYN, получатель отвечает пакетом SYN ACK, а затем отправитель отвечает пакетом ACK.

- Если получатель не отвечает на пакет SYN ACK после того, как отправитель отправляет пакет SYN, отправитель продолжает передавать пакет SYN в течение определенного времени или до истечения периода тайм-аута.
- Если получатель ответит на пакет SYN ACK после того, как отправитель отправит пакет SYN, но отправитель не ответит на пакет ACK, получатель продолжает передавать пакет SYN ACK в течение определенного времени или до истечения периода тайм-аута. (Это происходит в случае флуда SYN.)

11.3.3.2. Связанная конфигурация

Настройка тайм-аута TCP SYN

- Тайм-аут TCP SYN по умолчанию составляет 20 секунд.

- Запустите команду **ip tcp synwait-time** *seconds* в режиме глобальной конфигурации, чтобы настроить тайм-аут SYN в диапазоне от 5 до 300 секунд.
- В случае флуда SYN сокращение времени ожидания SYN снижает потребление ресурсов. Однако она не работает при непрерывном флуде SYN. Если устройство активно запрашивает подключение к внешнему устройству, например, с помощью telnet, сокращение времени ожидания SYN сокращает время ожидания пользователя. В плохой сети можно продлить время ожидания SYN.

ПРИМЕЧАНИЕ: в версии 11.0 или более поздней она применяется как к TCP IPv4, так и к TCP IPv6.

11.3.4. Настройка размера окна

11.3.4.1. Принцип работы

Данные из одноранговой узла кешируются в принимающем буфере TCP и затем считываются приложениями. Размер окна TCP указывает размер свободного места в принимающем буфере. Для подключения больших объемов данных с широкой полосой пропускания увеличение размера окна значительно повышает производительность передачи данных по протоколу TCP.

11.3.4.2. Связанная конфигурация

Настройка размера окна

- Запустите команду **ip tcp window-size** *size* в режиме глобальной конфигурации, чтобы настроить размер окна от 128 до (65 535<<14) байт. Значение по умолчанию — 65 535 байт. Если размер окна превышает 65 535 байт, увеличение окна будет включено автоматически.
- Размер окна, объявленный одноранговому узлу, является меньшим значением между настроенным размером окна и свободным пространством принимающего буфера.

ПРИМЕЧАНИЕ: в версии 11.0 или более поздней она применяется как к TCP IPv4, так и к TCP IPv6.

11.3.5. Настройка сброса отправки пакетов

11.3.5.1. Принцип работы

Если TCP-соединение, к которому принадлежит пакет, не может быть идентифицировано, то при передаче TCP-пакетов приложениям локальный конец отправляет пакет сброса на узел для прекращения TCP-соединения.

Злоумышленники могут использовать сообщения о недоступности порта для атаки на устройство.

11.3.5.2. Связанная конфигурация

Настройка отправки пакетов сброса TCP после получения сообщений о недоступности порта

По умолчанию включена функция отправки пакетов сброса TCP при получении сообщений о недоступности порта.

Выполните команду **no ip tcp send-reset** в режиме глобальной конфигурации, чтобы отключить отправку пакетов сброса TCP при получении сообщений о недоступности порта.

После включения этой функции злоумышленники могут использовать сообщения о недоступности порта для атаки на устройство.

ПРИМЕЧАНИЕ: в версии 11.0 или более поздней она применяется как к TCP IPv4, так и к TCP IPv6.

11.3.6. Настройка MSS

11.3.6.1. Принцип работы

MSS означает общий объем данных, содержащихся в сегменте TCP, за исключением параметров TCP.

Трехстороннее рукопожатие осуществляется посредством согласования MSS. Обе стороны добавляют опцию MSS к пакетам SYN, указывая на наибольший объем данных, который может обработать локальный конец, а именно, объем данных, разрешенных от однорангового узла. Обе стороны принимают MSS меньшего размера между ними, как объявленную MSS.

Значение MSS рассчитывается следующим образом:

- IPv4 TCP: MSS = размер заголовка исходящего интерфейса MTU IP (20 байт), размер заголовка TCP (20 байт).
- IPv6 TCP: MSS = размер заголовка IPv6 MTU пути (40 байт), размер заголовка TCP (20 байт).

ПРИМЕЧАНИЕ: в версии 11.0 или более поздней она применяется как к TCP IPv4, так и к TCP IPv6.

ПРИМЕЧАНИЕ: эффективная система MSS представляет собой меньшую систему между рассчитанной системой и сконфигурированной системой.

ПРИМЕЧАНИЕ: если соединение поддерживает определенные опции, то из значения MSS следует вычесть длину опции (с учетом смещения данных **data offset**). Например, 20 байт для дайджеста MD5 (с учетом смещения данных **data offset**) должны быть вычтены из MSS.

11.3.6.2. Связанная конфигурация

Настройка MSS

- Запустите команду **ip tcp mss** *max-segment-size* в режиме глобальной конфигурации, чтобы задать MSS. Диапазон составляет от 68 до 1000 байт. По умолчанию MSS рассчитывается на основе MTU. Если настроена система MSS, эффективная система представляет собой меньшую систему между рассчитанной системой и сконфигурированной системой.
- Слишком малая система MSS снижает производительность трансмиссии. Можно повысить передачу TCP, увеличив MSS. Выберите значение MSS, используя MTU интерфейса. Если первый больше, пакеты TCP будут фрагментированы, и производительность передачи будет снижена.

11.3.7. Обнаружение MTU пути

11.3.7.1. Принцип работы

Обнаружение MTU пути, предусмотренное в RFC1191, используется для обнаружения наименьшего MTU в пути TCP, чтобы избежать фрагментации и повысить коэффициент использования полосы пропускания сети. Процесс обнаружения MTU пути TCPv4 описан ниже.

- Источник отправляет TCP-пакеты с битом Don’t Fragment (DF), установленным во внешнем IP-заголовке.
- Если значение MTU исходящего интерфейса маршрутизатора в пути TCP меньше, чем длина IP-пакета, пакет будет удален, а пакет ошибок ICMP, передающий этот MTU, будет отправлен в источник.
- При анализе пакета ошибок ICMP источник получает наименьший MTU в пути (путь MTU).

Размер последующих сегментов данных, отправленных источником, не превысит MSS, который рассчитывается следующим образом: TCP MSS = Path MTU — размер заголовка IP — размер заголовка TCP.

11.3.7.2. Связанная конфигурация

Включение обнаружения MTU-пути

По умолчанию обнаружение MTU-пути отключено.

Запустите команду **ip tcp path-mtu-discovery**, чтобы включить PMTUD в режиме глобальной конфигурации. В версии 11.0 или более поздней она применяется только к протоколу IPv4 TCP. PMTUD TCPv6 включен постоянно и не может быть отключен.

11.3.8. TCP Keepalive

11.3.8.1. Принцип работы

Вы можете включить TCP keepalive, чтобы проверить, работает ли одноранговый узел нормально. Если TCP-конец не отправляет пакеты на другой конец в течение определенного периода времени (а именно периода бездействия), последний начинает несколько раз последовательно отправлять пакеты keepalive на первый. Если ответный пакет не получен, TCP-соединение считается неактивным, а затем закрытым.

11.3.8.2. Связанная конфигурация

Включение Keepalive

- По умолчанию TCP keepalive отключен.
- Запустите команду **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] в режиме глобальной конфигурации, чтобы включить TCP keepalive. Описание параметра см. в разделе Связанные команды.

ПРИМЕЧАНИЕ: в версии 11.0 или более поздней она применяется как к TCP IPv4, так и к TCP IPv6.

ПРИМЕЧАНИЕ: эта команда применяется как к серверу TCP, так и к клиенту.

11.4. Настройка

Настройка	Описание и команда	
Оптимизация производительности TCP	(ОПЦИОНАЛЬНО) используется для оптимизации производительности соединения TCP	
	ip tcp synwait-time	Настройка тайм-аута для соединения TCP
	ip tcp window-size	Настройка размера окна TCP
	ip tcp send-reset	Настройка отправки пакетов сброса TCP после получения сообщений, недоступных для порта
	ip tcp mss	Настройка системы MSS для подключения по протоколу TCP
	ip tcp path-mtu-discovery	Включает обнаружение MTU пути
Обнаружение исключения соединения TCP	(Необязательно) используется для определения того, работает ли одноранговый узел нормально	
	ip tcp keepalive	Включает TCP keepalive

11.4.1. Оптимизация производительности TCP

11.4.1.1. Результат конфигурации

Обеспечение оптимальной производительности TCP и предотвращение фрагментации.

11.4.1.2. Примечания

Недоступно

11.4.1.3. Этапы конфигурации

Настройка тайм-аута SYN

- Опционально.
- Настройте его на обоих концах соединения TCP.

Настройка размера окна TCP

- Опционально.
- Настройте его на обоих концах соединения TCP.

Настройка отправки пакетов сброса TCP после получения сообщений о недоступности порта.

- Опционально.

- Настройте его на обоих концах соединения TCP.

Настройка MSS

- Опционально.
- Настройте его на обоих концах соединения TCP.

Включение обнаружения MTU-пути

- Опционально.
- Настройте его на обоих концах соединения TCP.

11.4.1.4. Проверка конфигурации

Недоступно.

11.4.1.5. Связанные команды

Настройка тайм-аута SYN

Команда	**ip tcp synwait-time** *seconds*
Описание параметров	*seconds*: указывает время ожидания пакета SYN. Диапазон составляет от 5 до 300 секунд. По умолчанию: 20 секунд
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	В случае флуда SYN сокращение времени ожидания SYN снижает потребление ресурсов. Однако она не работает при непрерывном флуде SYN. Если устройство активно запрашивает подключение к внешнему устройству, например, с помощью telnet, сокращение времени ожидания SYN сокращает время ожидания пользователя. В плохой сети можно продлить время ожидания SYN

Настройка размера окна TCP

Команда	**ip tcp window-size** *size*
Описание параметров	*size*: указывает размер окна TCP. Диапазон составляет от 128 до (65 535 << 14) байт. Значение по умолчанию — 65 535 байт
Режим конфигурации	Режим глобальной конфигурации

Настройка отправки пакетов сброса TCP после получения сообщений о недоступности порта

Команда	**ip tcp send-reset**
Режим конфигурации	Режим глобальной конфигурации

Встроенная подсказка	По умолчанию включена функция отправки пакетов сброса TCP при получении сообщений о недоступности порта

Настройка MSS

Команда	**ip tcp mss** *max-segment-size*
Описание параметров	*max-segment-size*: указывает максимальный размер сегмента. Диапазон составляет от 68 до 10 000 байт. По умолчанию MSS рассчитывается на основе MTU
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Эта команда определяет MSS для установления связи TCP. Согласованная MSS для нового соединения должна быть меньше, чем MSS. Если вы хотите уменьшить MSS, выполните эту команду. В противном случае не выполняйте настройку

Настройка обнаружения MTU пути

Команда	**ip tcp path-mtu-discovery** [**age-timer** *minutes* **| age-timer infinite**]
Описание параметров	**age-timer** *minutes*: указывает интервал для нового пробирования после обнаружения MTU пути. Диапазон составляет от 10 до 30 минут. Значение по умолчанию — 10 минут. **age-timer infinite**: после обнаружения MTU пути пробирование не реализовывается
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	PMTUD — это алгоритм, описанный в RFC1191, направленный на повышение коэффициента использования полосы пропускания. При применении протокола TCP к пакетной передаче данных эта функция может способствовать повышению производительности передачи. Если MSS, используемая для подключения, меньше, чем может обработать одноранговое соединение, то MSS большего размера будет использоваться каждый раз, когда истечет время таймера. Таймер устаревания представляет собой временной интервал, в течение которого TCP оценивает MTU пути с помощью более крупной MSS. Процесс обнаружения останавливается, если либо система отправляемой MSS имеет такой же размер, как согласованная одноранговая сеть, либо пользователь отключил таймер на маршрутизаторе. Для отключения таймера установите его на **infinite**

11.4.1.6. Пример конфигурации

Включение обнаружения MTU пути

Этапы конфигурации	Включите PMTUD для соединения TCP. Выберите настройки таймера возраста по умолчанию
	QTECH# configure terminal QTECH(config)# ip tcp path-mtu-discovery QTECH(config)# end
Проверка конфигурации	Запустите команду **show tcp pmtu**, чтобы отобразить IPv4 TCP PMTU
	QTECH# show tcp pmtu Number Local Address Foreign Address PMTU 1 192.168.195.212.23 192.168.195.112.13560 1440
	Запустите команду **show ipv6 tcp pmtu**, чтобы отобразить IPv6 TCP PMTU
	QTECH# show ipv6 tcp pmtu Number Local Address Foreign Address PMTU 1 1000::1:23 1000::2.13560 1440

11.4.2. Обнаружение исключения соединения TCP

11.4.2.1. Результат конфигурации

Проверьте, работает ли одноранговый узел нормально.

11.4.2.2. Этапы конфигурации

Включение TCP Keepalive

- Опционально.

11.4.2.3. Связанные команды

Включение TCP Keepalive

Команда	**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]
Описание параметров	**interval** *num1*: указывает интервал отправки пакетов keepalive. Диапазон составляет от 1 до120 секунд. По умолчанию: 75 секунд. **times** *num2*: указывает максимальное время отправки пакетов keepalive. Диапазон составляет от 1 до 10. По умолчанию: 6.

	idle-period *num3*: указывает время, когда одноранговый узел не отправляет пакеты на локальный конец, оно составляет от 60 до 1800 секунд. Значение по умолчанию составляет 15 минут
Режим конфигурации	Режим глобальной конфигурации
Встроенная подсказка	Вы можете включить TCP keepalive, чтобы проверить, работает ли одноранговый узел нормально. Данная функция выключена по умолчанию. Предположим, что пользователь включает функцию keepalive TCP с настройками интервала, времени и периода бездействия по умолчанию. Пользователь не получает пакеты от другого конца в течение 15 минут, а затем начинает отправлять пакеты Keepalive каждые 75 секунд в течение 6 раз. Если пользователь не получает пакетов TCP, соединение TCP считается неактивным и затем закрывается

11.4.2.4. Пример конфигурации

Включение TCP Keepalive

Этапы конфигурации	Включите функцию keepalive TCP на устройстве с интервалом **interval** и периодом бездействия **idle-period**, установленным на 3 минуты и 60 секунд соответственно. Если после четырех попыток отправки пакетов keepalive пользователь не получает пакетов TCP с другого конца, соединение TCP считается неактивным
	QTECH# configure terminal QTECH(config)# ip tcp keepalive interval 60 times 4 idleperiod 180 QTECH(config)# end
Проверка конфигурации	Пользователь входит в систему устройства через telnet, а затем выключает локальное устройство. Запустите команду **show tcp connect** на удаленном устройстве, чтобы проверить, когда будет удалено соединение IPv4 TCP

11.5. Контроль состояния

11.5.1. Отображение

Описание	Команда
Отображение основной информации о соединении IPv4 TCP	**show tcp connect** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Отображение статистики соединения IPv4 TCP	**show tcp connect statistics**
Отображение MTU TCP IPv4	**show tcp pmtu** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Отображение информации о порте TCP IPv4	**show tcp port** [*num*]
Отображение основной информации о соединении IPv6 TCP	**show ipv6 tcp connect** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Отображение статистики соединения IPv6 TCP	**show ipv6 tcp connect statistics**
Отображение MTU TCP IPv6	**show ipv6 tcp pmtu** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Отображение информации о порте TCP IPv6	**show ipv6 tcp port** [*num*]

11.5.2. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Отображает отладочную информацию о TCPпакетах IPv4	**debug ip tcp packet** [**in** | **out**] [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global** | **vrf** *vrf-name*] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Отображает информацию по отладке соединения IPv4 TCP	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]

Описание	Команда
Отображает отладочную информацию о TCP-пакетах IPv6	**debug ipv6 tcp packet** [**in** | **out**] [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**global** | **vrf** *vrf-name*] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Отображает информацию по отладке соединения IPv6 TCP	**debug ipv6 tcp transactions** [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-port** *num*]

12. НАСТРОЙКА ПРОТОКОЛА IPV4/IPV6 REF

12.1. Обзор

На устройствах, которые не поддерживают аппаратную пересылку, пакеты IPv4/IPv6 пересылаются программно. Для оптимизации производительности пересылки на основе программного обеспечения, оборудование QTECH использует экспресс-пересылку IPv4/IPv6 с помощью функционала REF.

REF поддерживает две таблицы: Таблицу пересылки и таблицу смежности. Таблица пересылки используется для хранения информации о маршруте. Таблица смежности основана на таблице ARP и таблице соседей IPv6 и содержит информацию о перезаписи уровня 2 (MAC) для следующего перехода.

REF используется для активного разрешения next hop-ов и реализации балансировки нагрузки.

12.2. Применение

Применение	Описание
Балансировка нагрузки	Во время сетевой маршрутизации, когда префикс маршрута связан с несколькими следующими переходами, REF может реализовать балансировку нагрузки между несколькими следующими переходами

12.2.1. Балансировка нагрузки

12.2.1.1. Сценарий

Как показано на Рисунке 67, префикс маршрута связан с тремя next hop-ами на маршрутизаторе A, а именно: Link 1, Link 2 и Link 3. По умолчанию REF реализует балансировку нагрузки на основе IP-адреса назначения. Балансировка нагрузки может быть реализована также на основе IP-адреса источника и IP-адреса назначения.

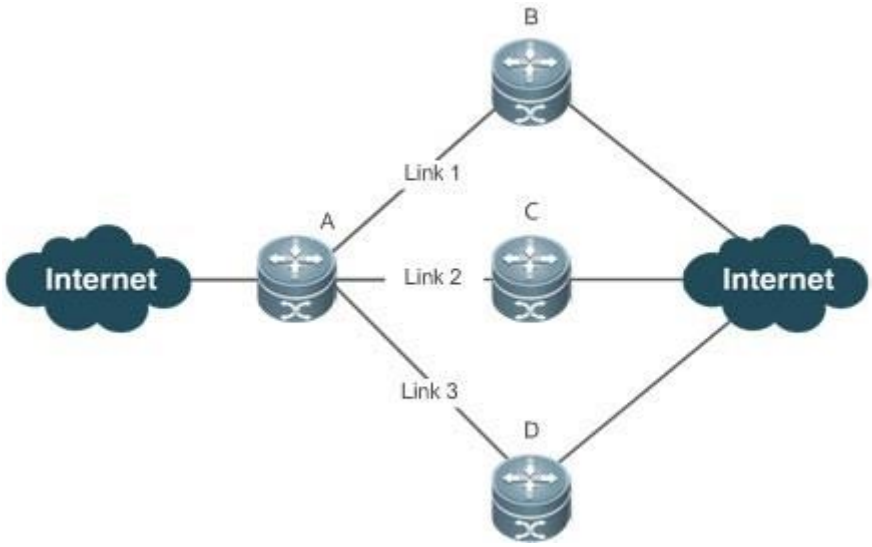


Рисунок 12-1.

A — это маршрутизатор, на котором выполняется REF.

B, C и D — передающие устройства.

12.2.1.2. Описание

Запустите REF на маршрутизаторе A.

12.3. Ключевые особенности

12.3.1. Базовые концепции

REF IPv4/IPv6 включает следующие основные понятия:

Таблица маршрутизации

В таблице маршрутизации IPv4/IPv6 содержатся маршруты к определенным местам назначения и сведения о топологии. Во время пересылки пакетов REF IPv4/IPv6 выбирает пути передачи пакетов в соответствии с таблицей маршрутизации.

Соседний узел

Соседний узел содержит информацию о выходном интерфейсе о маршрутизируемых пакетах, например, следующий переход, следующий обрабатываемый компонент и инкапсуляцию на уровне канала. Когда пакет сопоставлен с соседним узлом, пакет инкапсулируется и затем пересылается. Для запроса и обновления смежную таблицу узлов часто организуют в хештаблицу. Для поддержки балансировки нагрузки при маршрутизации информация о следующем переходе упорядочена в записи балансировки нагрузки. Соседний узел не может содержать информацию о next hop. Он может содержать индексы следующих компонентов (например, другие линейные карты и карты с несколькими сервисными картами), которые будут обрабатываться.

Активное разрешение

REF поддерживает разрешение следующего перехода. Если MAC-адрес следующего перехода неизвестен, REF будет активно разрешать следующий переход. IPv4 REF запрашивает разрешение следующего перехода для модуля ARP, а IPv6 REF применяет ND-модуль к разрешению.

Путь переадресации пакетов

Пакеты пересылаются на основе адресов IPv4/IPv6. Если указаны адреса IPv4/IPv6 источника и назначения пакета, определяется путь пересылки этого пакета.

12.3.2. Политики балансировки нагрузки

Балансировка нагрузки настроена на распределение нагрузки трафика между несколькими сетевыми каналами.

12.3.2.1. Принцип работы

По умолчанию коммутатор поддерживает политики балансировки нагрузки на основе IP-адресов назначения. В модели REF префикс маршрута связан с несколькими Next Hop, другими словами, это маршрут с несколькими путями. Маршрут будет связан с таблицей балансировки нагрузки и балансировкой нагрузки на основе веса. Если пакет IPv4/IPv6 соответствует записи балансировки нагрузки, основанной на самом длинном совпадении префиксов, REF выполняет расчет хэша на основе IPv4/IPv6-адреса пакета и выбирает путь для пересылки пакета.

12.4. Настройка

По умолчанию коммутатор поддерживает балансировку нагрузки на основе адресов назначения. Выполните следующие команды для контроля состояния.

12.4.1. Отображение статистики пакетов REF

Статистика REF-пакетов включает в себя количество пересылаемых пакетов и количество отброшенных пакетов по разным причинам. Можно определить, будут ли пакеты пересылаться в соответствии с ожиданиями, отобразив и очистив статистику REF-пакетов.

Команда	Описание
show ip ref packet statistics	Отображает статистику пакетов IPv4 REF
clear ip ref packet statistics	Удаляет статистику пакетов IPv4 REF
show ipv6 ref packet statistics	Отображает статистику пакетов IPv6 REF
clear ipv6 ref packet statistics	Удаляет статистику пакетов IPv6 REF

12.4.2. Отображение информации о смежности

Для отображения информации о смежности можно выполнить следующие команды:

Команда	Описание
show ip ref adjacency [**glean** | **local** | *ipaddress* | {**interface** *interface_type interface_number)* **| discard | statistics**]	Отображает удаленные смежности, локальные смежности, смежности указанного IP-адреса, смежности, связанные с указанным интерфейсом, и все смежные узлы в IPv4 REF
show ipv6 ref adjacency [glean | local | *ipv6-address* **| (interface** *interface_type interface_number*) **| discard | statistics**]	Отображает удаленные смежности, локальные смежности, смежности указанного адреса IPv6, смежности, связанные с указанным интерфейсом, и все смежные узлы в IPv6 REF

12.4.3. Отображение информации об активном разрешении

Для отображения Next Hop-ов, которые необходимо разрешить, можно выполнить следующие команды:

Команда	Описание
show ip ref resolve-list	Отображение следующего перехода для разрешения
show ipv6 ref resolve-list	Отображение Next Hop для разрешения

12.4.4. Отображение информации о пути переадресации пакетов

Пакеты пересылаются на основе адресов IPv4/IPv6. Если указаны адреса IPv4/IPv6 источника и назначения пакета, определяется путь пересылки этого пакета. Выполните

следующие команды и укажите адреса источника и назначения IPv4/IPv6 пакета. Отображается путь пересылки пакета, например, пакет отбрасывается, отправляется на ЦП или пересылается. Кроме того, отображается интерфейс, который пересылает пакет.

Команда	Описание
show ip ref exact-route [**oob** | **vrf** *vrf_name*] *source-ipaddress dest_ipaddress*	Отображает путь пересылки пакета. oob указывает внеполосную сеть управления
show ipv6 ref exact-route [**oob** | **vrf** *vrf-name*] *src-ipv6-address dst-ipv6-address*	Отображает путь пересылки пакета IPv6. oob указывает внеполосную сеть управления

12.4.5. Отображение информации о маршруте в таблице REF

Для отображения информации о маршруте в таблице REF выполните следующие команды:

Команда	Описание
show ip ref route [**vrf** *vrf_name*] [**default** | {*ip mask*}| **statistics**]	Отображение информации о маршруте в таблице REF IPv4. Параметр **default** указывает маршрут по умолчанию
show ipv6 ref route [**vrf** *vrf-name*] [**default** | **statistics** | *prefix/len*]	Отображение информации о маршруте в таблице REF IPv6. Параметр **default** указывает маршрут по умолчанию

13. ОБЩАЯ ИНФОРМАЦИЯ

13.1. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

13.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться разделом технической поддержки пользователей QTECH на нашем сайте www.qtech.ru/support/.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

13.3. Электронная версия документа

Дата публикации 28.02.2025

https://files.qtech.ru/upload/switchers/QSW-6300/QSW-6300_ip_address_app_config_guide.pdf