

Руководство по настройке
Конфигурация безопасности
Ethernet-коммутаторы агрегации
серия QSW-4700

Оглавление

1. НАСТРОЙКА AAA 17
1.1. Обзор 17
1.2. Приложения 17
1.2.1. Настройка AAA в однодоменной среде 18
1.2.1.1. Сценарий 18
1.2.1.2. Развертывание 18
1.2.2. Настройка AAA в многодоменной среде 19
1.2.2.1. Сценарий 19
1.2.2.2. Развертывание 19
1.3. Функции 19
1.3.1. Базовые концепты 19
1.3.1.1. Обзор 21
1.3.2. AAA-аутентификация 22
1.3.2.1. Схема аутентификации AAA 22
1.3.2.2. Связанная конфигурация 23
1.3.3. Авторизация AAA 23
1.3.3.1. Связанная конфигурация 24
1.3.4. Учет AAA 24
1.3.4.1. Связанная конфигурация 25
1.3.5. Мультидоменный AAA 25
1.3.5.1. Связанная конфигурация 26
1.3.6. Переключатель входа в систему для slave-устройства AAA 26
1.3.6.1. Связанная конфигурация 26
1.3.7. Кеширование результатов авторизации 27
1.3.7.1. Связанная конфигурация 27
1.3.8. Настройка аутентификации AAA 30
1.3.8.1. Эффект конфигурации 30
1.3.8.2. Примечания 30
1.3.8.3. Шаги настройки 31
1.3.8.4. Проверка 32
1.3.8.5. Связанные команды 32
1.3.8.6. Пример конфигурации 35
1.3.8.7. Распространенные ошибки 38
1.3.9. Настройка авторизации AAA 38
1.3.9.1. Эффект конфигурации 38
1.3.9.2. Примечания 38

1.3.9.3. Шаги настройки 38
1.3.9.4. Проверка 39
1.3.9.5. Связанные команды 39
1.3.9.6. Пример конфигурации 42
1.3.10. Настройка учета AAA 47
1.3.10.1. Эффект конфигурации 47
1.3.10.2. Примечания 47
1.3.10.3. Шаги настройки 48
1.3.10.4. Проверка 49
1.3.10.5. Связанные команды 49
1.3.10.6. Пример конфигурации 52
1.3.11. Настройка группы серверов AAA 55
1.3.11.1. Эффект конфигурации 55
1.3.11.2. Примечания 55
1.3.11.3. Шаги настройки 55
1.3.11.4. Проверка 56
1.3.11.5. Связанные команды 56
1.3.11.6. Пример конфигурации 57
1.3.11.7. Распространенные ошибки 58
1.3.12. Настройка службы AAA на основе домена 59
1.3.12.1. Эффект конфигурации 59
1.3.12.2. Примечания 59
1.3.12.3. Шаги настройки 59
1.3.12.4. Проверка 60
1.3.12.5. Связанные команды 61
1.3.12.6. Пример конфигурации 63
1.3.13. Настройка переключателя входа в систему для slave-устройства AAA 65
1.3.13.1. Эффект конфигурации 65
1.3.13.2. Примечания 65
1.3.13.3. Шаги настройки 65
1.3.13.4. Проверка 65
1.3.13.5. Связанные команды 66
1.3.13.6. Пример конфигурации 66
1.3.14. Настройка кеширования результатов авторизации 66
1.3.14.1. Эффект конфигурации 66
1.3.14.2. Примечания 67
1.3.14.3. Шаги настройки 67
1.3.14.4. Проверка 67

1.3.14.5. Связанные команды 67
1.3.14.6. Пример конфигурации 67
1.4. Мониторинг 68
1.4.1. Очистка 68
1.4.2. Отображение 68
2. НАСТРОЙКА RADIUS 69
2.1. Обзор 69
2.1.1. Протоколы и стандарты 69
2.2. Приложения 70
2.2.1. Предоставление услуг аутентификации, авторизации и учета для пользователей доступа 70
2.2.1.1. Сценарий 70
2.2.1.2. Развертывание 70
2.2.2. Принуждение пользователей к отключению от сети 71
2.2.2.1. Сценарий 71
2.2.2.2. Развертывание 71
2.3. Функции 71
2.3.1. Базовые концепты 71
2.3.2. Обзор 77
2.3.3. RADIUS-аутентификация, авторизация и учет 77
2.3.3.1. Принцип работы 78
2.3.3.2. Связанная конфигурация 79
2.3.4. Исходный адрес пакетов RADIUS 79
2.3.4.1. Принцип работы 79
2.3.4.2. Связанная конфигурация 79
2.3.5. Тайм-аут повторной передачи RADIUS 80
2.3.5.1. Принцип работы 80
2.3.5.2. Связанная конфигурация 80
2.3.6. Обнаружение доступности сервера RADIUS 80
2.3.6.1. Принцип работы 80
2.3.6.2. Связанная конфигурация 80
2.3.7. Принудительный автономный режим RADIUS 81
2.3.7.1. Принцип работы 81
2.3.7.2. Связанная конфигурация 81
2.4. Конфигурация 81
2.4.1. Базовая конфигурация RADIUS 83
2.4.1.1. Эффект конфигурации 83
2.4.1.2. Примечания 83

2.4.1.3. Шаги настройки 83
2.4.1.4. Проверка 84
2.4.1.5. Связанные команды 84
2.4.1.6. Пример конфигурации 86
2.4.1.7. Распространенные ошибки 88
2.4.2. Настройка типа атрибута RADIUS 88
2.4.2.1. Эффект конфигурации 88
2.4.2.2. Примечания 88
2.4.2.3. Шаги настройки 88
2.4.2.4. Проверка 89
2.4.2.5. Связанные команды 89
2.4.2.6. Пример конфигурации 90
2.4.3. Настройка обнаружения доступности RADIUS 90
2.4.3.1. Эффект конфигурации 90
2.4.3.2. Примечания 91
2.4.3.3. Шаги настройки 91
2.4.3.4. Проверка 92
2.4.3.5. Связанные команды 92
2.4.3.6. Пример конфигурации 93
2.5. Мониторинг 94
2.5.1. Очистка 94
2.5.2. Отображение 94
2.5.3. Отладка 94
3. НАСТРОЙКА TACACS+ 96
3.1. Обзор 96
3.1.1. Протоколы и стандарты 96
3.2. Приложения 96
3.2.1. Управление и контроль входа конечных пользователей 96
3.2.1.1. Сценарий 96
3.2.1.2. Развертывание 96
3.3. Функции 97
3.3.1. Базовые концепты 97
3.3.2. Обзор 97
3.3.3. TACACS+ Аутентификация, авторизация и учет 98
3.3.3.1. Принцип работы 98
3.4. Конфигурация 99
3.4.1. Настройка основных функций TACACS+ 100

3.4.1.1. Эффект конфигурации 100
3.4.1.2. Примечания 100
3.4.1.3. Шаги настройки 100
3.4.1.4. Проверка 102
3.4.1.5. Пример конфигурации 103
3.4.1.6. Распространенные ошибки 103
3.4.2. Настройка раздельной обработки аутентификации, авторизации и учета TACACS+ 104
3.4.2.1. Эффект конфигурации 104
3.4.2.2. Примечания 104
3.4.2.3. Шаги настройки 104
3.4.2.4. Проверка 106
3.4.2.5. Пример конфигурации 106
3.4.2.6. Распространенные ошибки 108
3.5. Мониторинг 108
3.5.1. Отображение 108
3.5.2. Отладка 108
4. КОНФИГУРАЦИЯ SCC 109
4.1. Обзор 109
4.2. Приложение 109
4.2.1. Контроль доступа к расширенным кампусным сетям уровня 2 109
4.2.1.1. Сценарий 109
4.2.1.2. Развертывание 110
4.2.1.3. Базовые концепты 111
4.2.1.4. Функции 112
4.2.2. Режим аутентификации 112
4.2.2.1. Принцип работы 112
4.2.3. VLAN с освобождением от аутентификации 113
4.2.3.1. Принцип работы 113
4.2.4. Количество пользователей IPv4 113
4.2.4.1. Принцип работы 113
4.2.5. Миграция аутентифицированных пользователей 114
4.2.5.1. Принцип работы 114
4.2.6. Обнаружение онлайн-статуса пользователя 115
4.2.6.1. Принцип работы 115
4.3. Конфигурация 115
4.3.1. Настройка режима аутентификации 116
4.3.1.1. Эффект конфигурации 116

4.3.1.2. Меры предосторожности 116
4.3.1.3. Метод конфигурации 117
4.3.1.4. Проверка 117
4.3.1.5. Примеры конфигурации 117
4.3.2. Настройка VLAN с освобождением от аутентификации 119
4.3.2.1. Эффект конфигурации 119
4.3.2.2. Уведомления 119
4.3.2.3. Шаги настройки 119
4.3.2.4. Проверка 119
4.3.2.5. Примеры конфигурации 120
4.3.3. Настройка количества пользователей IPv4 122
4.3.3.1. Эффект конфигурации 122
4.3.3.2. Метод конфигурации 122
4.3.3.3. Проверка 122
4.3.3.4. Примеры конфигурации 123
4.3.4. Настройка миграции авторизованных пользователей 124
4.3.4.1. Эффект конфигурации 124
4.3.4.2. Меры предосторожности 124
4.3.4.3. Метод конфигурации 125
4.3.4.4. Проверка 125
4.3.4.5. Примеры конфигурации 125
4.3.5. Настройка определения онлайн-статуса пользователя 126
4.3.5.1. Эффект конфигурации 126
4.3.5.2. Меры предосторожности 127
4.3.5.3. Метод конфигурации 127
4.3.5.4. Проверка 128
4.3.5.5. Примеры конфигурации 128
4.4. Мониторинг 129
4.4.1. Отображение 129
4.4.2. Отладка 129
5. НАСТРОЙКА ПОЛИТИКИ ПАРОЛЕЙ 130
5.1. Обзор 130
5.2. Функции 130
5.2.1. Базовые концепты 130
5.3. Конфигурация 131
5.3.1. Настройка политики безопасности паролей 131
5.3.1.1. Сетевые требования 131

5.3.1.2. Примечания 131
5.3.1.3. Шаги настройки 132
5.3.1.4. Проверка 132
5.3.1.5. Связанные команды 132
5.3.1.6. Примеры конфигурации 134
5.3.1.7. Распространенные ошибки 136
5.4. Мониторинг 136
5.4.1. Отображение 136
6. НАСТРОЙКА STORM CONTROL 137
6.1. Обзор 137
6.2. Приложения 137
6.2.1. Предотвращение сетевых атак 137
6.2.1.1. Сценарий 137
6.2.1.2. Развертывание 137
6.3. Функции 138
6.3.1. Базовые концепты 138
6.3.2. Обзор 138
6.3.3. Storm Control одноадресных пакетов 138
6.3.3.1. Принцип работы 139
6.3.3.2. Связанная конфигурация 139
6.3.4. Storm Control многоадресных пакетов 139
6.3.4.1. Принцип работы 139
6.3.4.2. Связанная конфигурация 139
6.3.5. Storm Control широковещательных пакетов 139
6.3.5.1. Принцип работы 139
6.3.5.2. Связанная конфигурация 140
6.4. Конфигурация 140
6.4.1. Настройка основных функций Storm Control 140
6.4.1.1. Эффект конфигурации 140
6.4.1.2. Примечания 140
6.4.1.3. Шаги настройки 140
6.4.1.4. Проверка 141
6.4.1.5. Связанные команды 141
6.4.1.6. Пример конфигурации 142
6.5. Мониторинг 143
6.5.1. Отображение 143

7. НАСТРОЙКА SSH 144
7.1. Обзор 144
7.1.1. Протоколы и стандарты 144
7.2. Приложения 144
7.2.1. Управление SSH-устройствами 145
7.2.1.1. Сценарий 145
7.2.1.2. Развертывание 145
7.2.2. Аутентификация по локальной учетной записи SSH 146
7.2.2.1. Сценарий 146
7.2.2.2. Развертывание 146
7.2.3. Аутентификация SSH AAA 147
7.2.3.1. Сценарий 147
7.2.3.2. Развертывание 147
7.2.4. Аутентификация с открытым ключом SSH 147
7.2.4.1. Сценарий 147
7.2.4.2. Развертывание 148
7.2.5. Передача файлов SSH 148
7.2.5.1. Сценарий 148
7.2.5.2. Развертывание 148
7.2.6. SSH-клиентское приложение 148
7.2.6.1. Сценарий 148
7.2.6.2. Развертывание 148
7.3. Функции 149
7.3.1. Базовые концепты 149
7.3.2. Обзор 150
7.3.3. SSH-сервер 150
7.3.3.1. Принцип работы 150
7.3.3.2. Связанная конфигурация 151
7.3.4. Служба SCP 152
7.3.4.1. Принцип работы 152
7.3.4.2. Связанная конфигурация 153
7.3.5. SSH-клиент 153
7.3.5.1. Принцип работы 153
7.3.5.2. Связанная конфигурация 153
7.3.6. SCP-клиент 153
7.3.6.1. Принцип работы 153
7.3.6.2. Связанная конфигурация 154
7.4. Конфигурация 154

7.4.1. Настройка SSH-сервера 155
7.4.1.1. Эффект конфигурации 155
7.4.1.2. Примечания 156
7.4.1.3. Шаги настройки 156
7.4.1.4. Проверка 157
7.4.1.5. Связанные команды 157
7.4.1.6. Пример конфигурации 162
7.4.1.7. Распространенные ошибки 183
7.4.2. Настройка службы SCP 183
7.4.2.1. Эффект конфигурации 183
7.4.2.2. Примечания 183
7.4.2.3. Шаги настройки 183
7.4.2.4. Проверка 184
7.4.2.5. Связанные команды 184
7.4.2.6. Пример конфигурации 184
7.4.3. Настройка SSH-клиента 185
7.4.3.1. Эффект конфигурации 185
7.4.3.2. Примечания 186
7.4.3.3. Шаги настройки 186
7.4.3.4. Проверка 186
7.4.3.5. Связанные команды 186
7.4.3.6. Пример конфигурации 189
7.4.4. Настройка SCP-клиента 192
7.4.4.1. Эффект конфигурации 192
7.4.4.2. Примечания 192
7.4.4.3. Шаги настройки 192
7.4.4.4. Проверка 192
7.4.4.5. Связанные команды 192
7.4.4.6. Пример конфигурации 194
7.5. Мониторинг 197
7.5.1. Отображение 197
7.5.2. Отладка 197
8. НАСТРОЙКА URPF 198
8.1. Обзор 198
8.1.1. Протоколы и стандарты 198
8.2. Приложения 198
8.2.1. Строгий режим 198

8.2.1.1. Сценарий 198
8.2.1.2. Развертывание 199
8.2.2. Свободный режим 199
8.2.2.1. Сценарий 199
8.2.2.2. Развертывание 200
8.3. Функции 200
8.3.1. Базовые концепты 200
8.3.2. Обзор 201
8.3.3. Включение URPF 201
8.3.3.1. Принцип работы 201
8.3.3.2. Связанная конфигурация 202
8.3.4. Уведомление о коэффициенте потери пакетов URPF 202
8.3.4.1. Принцип работы 202
8.3.4.2. Связанная конфигурация 203
8.4. Конфигурация 203
8.4.1. Включение URPF 203
8.4.1.1. Эффект конфигурации 203
8.4.1.2. Примечания 203
8.4.1.3. Шаги настройки 203
8.4.1.4. Проверка 203
8.4.1.5. Связанные команды 204
8.5. Мониторинг 205
8.5.1. Очистка 205
8.5.2. Отображение 205
8.5.3. Отладка 205
9. НАСТРОЙКА CPP 207
9.1. Обзор 207
9.2. Приложения 207
9.2.1. Предотвращение вредоносных атак 207
9.2.1.1. Сценарий 207
9.2.1.2. Развертывание 208
9.2.2. Предотвращение узких мест при обработке центральным процессором 208
9.2.2.1. Сценарий 208
9.2.2.2. Развертывание 208
9.3. Функции 209
9.3.1. Базовые концепты 209
9.3.2. Обзор 209

9.3.3. Классификатор 210
9.3.3.1. Принцип работы 210
9.3.4. Измеритель 210
9.3.4.1. Принцип работы 210
9.3.4.2. Связанная конфигурация 211
9.3.5. Очередь 211
9.3.5.1. Принцип работы 211
9.3.5.2. Связанная конфигурация 211
9.3.6. Диспетчер 211
9.3.6.1. Принцип работы 211
9.3.7. Шейпер 211
9.3.7.1. Принцип работы 211
9.3.7.2. Связанная конфигурация 212
9.4. Конфигурация 212
9.4.1. Настройка CPP 213
9.4.1.1. Эффект конфигурации 213
9.4.1.2. Примечания 213
9.4.1.3. Шаги настройки 213
9.4.1.4. Проверка 214
9.4.1.5. Связанные команды 214
9.4.1.6. Пример конфигурации 215
9.4.2. Настройка предупреждения CPP 218
9.4.2.1. Эффект конфигурации 218
9.4.2.2. Шаги настройки 219
9.4.2.3. Связанные команды 219
9.4.2.4. Пример конфигурации 220
9.5. Мониторинг 220
9.5.1. Очистка 220
9.5.2. Отображение 221
10. НАСТРОЙКА DHCP SNOOPING 222
10.1. Обзор 222
10.1.1. Протоколы и стандарты 222
10.2. Приложения 222
10.2.1. Защита от спуфинга службы DHCP 222
10.2.1.1. Сценарий 222
10.2.1.2. Развертывание 223
10.2.2. Защита от флудинга DHCP-пакетов 223

10.2.2.1. Сценарий 223
10.2.2.2. Развертывание 223
10.2.3. Защита от поддельных пакетов DHCP 224
10.2.3.1. Сценарий 224
10.2.3.2. Развертывание 224
10.2.4. Защита от спуфинга IP/MAC 225
10.2.4.1. Сценарий 225
10.2.4.2. Развертывание 225
10.2.5. Предотвращение аренды IP-адресов 225
10.2.5.1. Сценарий 225
10.2.5.2. Развертывание 226
10.2.6. Обнаружение ARP-атак 226
10.2.6.1. Сценарий 226
10.2.6.2. Развертывание 226
10.3. Функции 226
10.3.1. Базовые концепты 226
10.3.2. Обзор 228
10.3.3. Фильтрация пакетов DHCP 228
10.3.3.1. Принцип работы 228
10.3.3.2. Связанная конфигурация 229
10.3.4. Создание базы данных привязок DHCP Snooping 229
10.3.4.1. Принцип работы 229
10.3.4.2. Связанная конфигурация 229
10.4. Конфигурация 230
10.4.1. Настройка основных функций DHCP Snooping 231
10.4.1.1. Эффект конфигурации 231
10.4.1.2. Примечания 231
10.4.1.3. Шаги настройки 231
10.4.1.4. Проверка 232
10.4.1.5. Связанные команды 232
10.4.1.6. Пример конфигурации 235
10.4.1.7. Распространенные ошибки 236
10.4.2. Настройка Option82 236
10.4.2.1. Эффект конфигурации 236
10.4.2.2. Примечания 237
10.4.2.3. Шаги настройки 237
10.4.2.4. Проверка 237
10.4.2.5. Связанные команды 237

10.4.2.6. Пример конфигурации 238
10.5. Мониторинг 239
10.5.1. Очистка 239
10.5.2. Отображение 239
10.5.3. Отладка 239
11. НАСТРОЙКА NFPP 240
11.1. Обзор 240
11.2. Приложения 240
11.2.1. Ограничение скорости атаки 240
11.2.1.1. Сценарий 240
11.2.1.2. Развертывание 241
11.2.2. Централизованное распределение пропускной способности 241
11.2.2.1. Сценарий 241
11.2.2.2. Развертывание 242
11.3. Функции 242
11.3.1. Базовые концепты 242
11.3.2. Обзор 244
11.3.3. Ограничение скорости на основе хоста и идентификация атак 244
11.3.3.1. Принцип работы 245
11.3.3.2. Связанные настройки 245
11.3.4. Ограничение скорости на основе портов и идентификация атак 246
11.3.4.1. Принцип работы 246
11.3.4.2. Связанная конфигурация 246
11.3.5. Период мониторинга 246
11.3.5.1. Принцип работы 246
11.3.5.2. Связанная конфигурация 246
11.3.6. Период изоляции 247
11.3.6.1. Принцип работы 247
11.3.6.2. Связанная конфигурация 247
11.3.7. Доверенные хосты 248
11.3.7.1. Принцип работы 248
11.3.7.2. Связанная конфигурация 248
11.3.8. Централизованное распределение пропускной способности 248
11.3.8.1. Принцип работы 248
11.3.8.2. Связанная конфигурация 249
11.4. Конфигурация 249
11.4.1. Настройка ARP Guard 254

11.4.1.1. Эффект конфигурации 254
11.4.1.2. Примечания 255
11.4.1.3. Шаги настройки 255
11.4.1.4. Проверка 257
11.4.1.5. Связанные команды 257
11.4.1.6. Пример конфигурации 260
11.4.2. Настройка IP Guard 261
11.4.2.1. Эффект конфигурации 261
11.4.2.2. Примечания 262
11.4.2.3. Шаги настройки 262
11.4.2.4. Проверка 264
11.4.2.5. Связанные команды 264
11.4.2.6. Пример конфигурации 267
11.4.3. Настройка ICMP Guard 268
11.4.3.1. Эффект конфигурации 268
11.4.3.2. Примечания 269
11.4.3.3. Шаги настройки 269
11.4.3.4. Проверка 270
11.4.3.5. Связанные команды 271
11.4.3.6. Пример конфигурации 274
11.4.4. Настройка DHCP Guard 275
11.4.4.1. Эффект конфигурации 275
11.4.4.2. Примечания 275
11.4.4.3. Шаги настройки 276
11.4.4.4. Проверка 277
11.4.4.5. Связанные команды 277
11.4.4.6. Пример конфигурации 280
11.4.5. Настройка DHCPv6 Guard 281
11.4.5.1. Эффект конфигурации 281
11.4.5.2. Примечания 281
11.4.5.3. Шаги настройки 281
11.4.5.4. Проверка 282
11.4.5.5. Связанные команды 283
11.4.5.6. Пример конфигурации 285
11.4.6. Настройка ND Guard 286
11.4.6.1. Эффект конфигурации 286
11.4.6.2. Примечания 286
11.4.6.3. Шаги настройки 286

11.4.6.4. Проверка 287
11.4.6.5. Связанные команды 287
11.4.6.6. Пример конфигурации 289
11.4.7. Настройка Self-Defined Guard 289
11.4.7.1. Эффект конфигурации 289
11.4.7.2. Примечания 289
11.4.7.3. Шаги настройки 289
11.4.7.4. Проверка 294
11.4.7.5. Связанные команды 295
11.4.7.6. Пример конфигурации 298
11.4.8. Настройка централизованного распределения полосы пропускания 299
11.4.8.1. Эффект конфигурации 299
11.4.8.2. Примечания 299
11.4.8.3. Шаги настройки 300
11.4.8.4. Проверка 300
11.4.8.5. Связанные команды 300
11.4.8.6. Пример конфигурации 300
11.4.9. Настройка ведения журнала NFPP 301
11.4.9.1. Эффект конфигурации 301
11.4.9.2. Примечания 301
11.4.9.3. Шаги настройки 301
11.4.9.4. Проверка 302
11.4.9.5. Связанные команды 302
11.4.9.6. Пример конфигурации 303
11.5. Мониторинг 304
11.5.1. Очистка 304
11.5.2. Отображение 304
12. ОБЩАЯ ИНФОРМАЦИЯ 306
12.1. Гарантия и сервис 306
12.2. Техническая поддержка 306
12.3. Электронная версия документа 306

1. НАСТРОЙКА AAA

1.1. Обзор

Аутентификация, авторизация и учет (AAA) обеспечивают единую структуру для настройки служб идентификации, авторизации и учета. Сетевые устройства QTECH поддерживают приложение AAA.

AAA предоставляет следующие услуги по модульному принципу:

Аутентификация: относится к проверке личности пользователя для доступа к сети и сетевых услуг. Аутентификация подразделяется на локальную аутентификацию и аутентификацию с помощью службы удаленной аутентификации пользователей по телефонной линии (RADIUS) и системы управления доступом терминала контроллера доступа + (TACACS+).

Авторизация: относится к предоставлению определенных сетевых услуг пользователям в соответствии с рядом определенных пар атрибут-значение (AV). Пары описывают, какие операции разрешено выполнять пользователям. Пары AV хранятся на серверах сетевого доступа (NAS) или удаленных серверах аутентификации.

Учет: относится к отслеживанию потребления ресурсов пользователями. Когда учет включен, NAS собирают статистику использования сетевых ресурсов пользователями и отправляют их в парах AV на серверы аутентификации. Записи будут храниться на серверах аутентификации и могут быть прочитаны и проанализированы специальным программным обеспечением для реализации учета, статистики и отслеживания использования сетевых ресурсов.

AAA является наиболее фундаментальным методом контроля доступа. Сетевые устройства QTECH также предоставляют другие простые функции контроля доступа, такие как аутентификация по локальному имени пользователя и онлайн-аутентификация по паролю. По сравнению с ними, AAA предлагает более высокий уровень сетевой безопасности.

AAA имеет следующие преимущества:

- Надежная гибкость и управляемость
- Масштабируемость
- Стандартная аутентификация
- Несколько резервных систем

1.2. Приложения

Приложение	Описание
Настройка AAA в однодоменной среде	AAA выполняется для всех пользователей в одном домене
Настройка AAA в многодоменной среде	AAA выполняется для пользователей в разных доменах с использованием разных методов

1.2.1. Настройка AAA в однодоменной среде

1.2.1.1. Сценарий

В сетевом сценарии, показанном на Рисунке 1-1, для улучшения управления безопасностью на NAS должны быть выполнены следующие требования к приложению:

1. Чтобы упростить управление учетными записями и избежать раскрытия информации, у каждого администратора есть отдельная учетная запись с разными именами пользователя и паролем.
2. Пользователи должны пройти аутентификацию перед доступом к NAS. Аутентификация может быть в локальном или централизованном режиме. Рекомендуется комбинировать два режима, с централизованным режимом в качестве активного и локальным режимом в качестве резервного. В результате пользователи должны сначала пройти аутентификацию на сервере RADIUS. Если сервер RADIUS не отвечает, он переходит к локальной аутентификации.
3. В процессе аутентификации пользователи могут быть классифицированы и ограничены в доступе к различным NAS.
4. Управление разрешениями: управляемые пользователи делятся на суперпользователей и обычных пользователей. Суперпользователи имеют право просматривать и настраивать NAS, а обычные пользователи могут только просматривать конфигурацию NAS.
5. Записи пользователей AAA хранятся на серверах, и их можно просматривать и использовать для аудита. (Сервер TACACS+ в этом примере выполняет учет.)

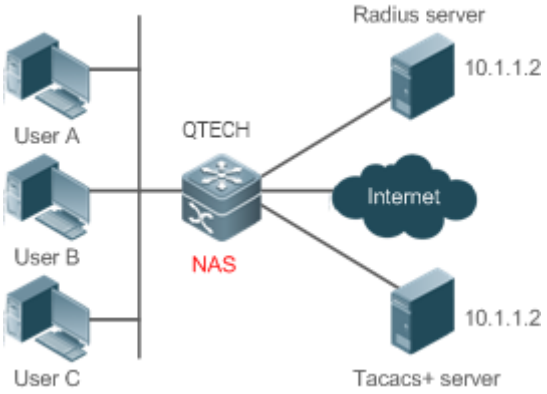


Рисунок 1-1.

Пользователь A, пользователь B и Пользователь C подключаются к NAS проводным или беспроводным способом.

NAS — это коммутатор доступа или конвергенции.

Сервер RADIUS может быть Windows Server (IAS), системным компонентом UNIX или программным обеспечением выделенного сервера, предоставленным поставщиком.

Сервер TACACS+ может быть выделенным серверным программным обеспечением, предоставленным поставщиком.

1.2.1.2. Развертывание

- Включите AAA на NAS.
- Настройте сервер аутентификации на NAS.
- Настройте локальных пользователей на NAS.

- Настройте службу аутентификации на NAS.
- Настройте службу авторизации на NAS.
- Настройте службу учета на NAS.

1.2.2. Настройка AAA в многодоменной среде

1.2.2.1. Сценарий

Настройте службу AAA на основе домена на NAS.

- Пользователь может войти в систему, введя имя пользователя PC1@QTECH.ru или PC2@QTECH.ru и правильный пароль на клиенте 802.1X.
- Управление разрешениями: управляемые пользователи делятся на суперпользователей и обычных пользователей. Суперпользователи имеют право просматривать и настраивать NAS, а обычные пользователи могут только просматривать конфигурацию NAS.
- Записи пользователей AAA хранятся на серверах, и их можно просматривать и использовать для аудита.

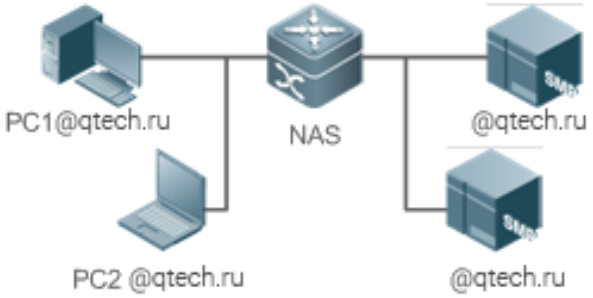


Рисунок 1-2.

Клиенты с именами пользователей PC1@qtech.ru и PC2@qtech.ru подключаются к NAS проводным или беспроводным способом.

NAS — это коммутатор доступа или конвергенции.

Сервер Security Accounts Manager (SAM) — это универсальный сервер RADIUS.

1.2.2.2. Развертывание

- Включите AAA на NAS.
- Настройте сервер аутентификации на NAS.
- Настройте локальных пользователей на NAS.
- Определите список методов AAA на NAS.
- Включите AAA на основе домена на NAS.
- Создайте домены и антивирусные наборы на NAS.

1.3. Функции

1.3.1. Базовые концепты

Локальная аутентификация и аутентификация на удаленном сервере

Локальная аутентификация — это процесс, при котором введенные пароли проверяются базой данных на NAS.

Аутентификация удаленного сервера — это процесс, в котором введенные пароли проверяются по базе данныхна удаленном сервере. В основном это реализовано сервером RADIUS и сервером TACACS+.

Список методов

AAA реализуется с использованием различных методов безопасности. Список методов определяет последовательность реализации метода. Список методов может содержать один или несколько протоколов безопасности, чтобы резервный метод мог взять на себя службу AAA в случае сбоя первого метода. На устройствах QTECH сначала пробуется первый метод в списке, а затем один за другим пробуются следующие, если предыдущий не дает ответа. Этот процесс выбора метода продолжается до тех пор, пока метод безопасности не ответит или все методы безопасности в списке не будут опробованы. Аутентификация завершается ошибкой, если ни один из методов в списке не отвечает.

Список методов содержит ряд методов безопасности, которые будут последовательно запрашиваться для проверки личности пользователя. Он позволяет определить один или несколько протоколов безопасности, используемых для аутентификации, чтобы резервный метод аутентификации брал на себя функции в случае сбоя активного метода безопасности. На устройствах QTECH сначала пробуется первый метод в списке, а затем один за другим пробуются следующие, если предыдущий не дает ответа. Этот процесс выбора метода продолжается до тех пор, пока метод не ответит или все методы в списке методов не будут опробованы. Аутентификация завершается ошибкой, если ни один из методов в списке не отвечает.

ПРИМЕЧАНИЕ: следующий метод аутентификации применяется на устройствах QTECH только в том случае, если текущий метод не отвечает. Когда метод отказывает пользователю в доступе, процесс идентификации завершается без использования других методов.

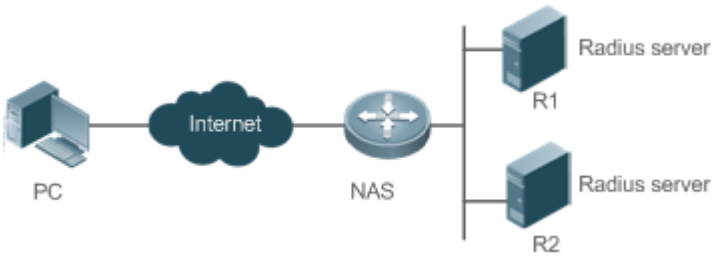


Рисунок 1-3.

Рисунок 1-3 показывает типичную топологию сети AAA, в которой развернуты два сервера RADIUS (R1 и R2) и один NAS. NAS может быть клиентом для серверов RADIUS.

Предположим, что системный администратор определяет список методов, где NAS последовательно выбирает маршрутизаторы R1 и R2 для получения идентификационной информации пользователя, а затем обращается к локальной базе данных имен пользователей на сервере. Например, когда удаленный пользователь ПК инициирует dial-up-доступ, NAS сначала запрашивает личность пользователя на маршрутизаторе R1. Когда аутентификация на R1 завершена, R1 возвращает ответ «Принять» (Accept) на NAS. Затем пользователю разрешается доступ в Интернет. Если R1 возвращает ответ «Отклонить» (Reject), пользователю будет отказано в доступе в Интернет, и соединение будет разорвано. Если R1 не отвечает, NAS считает, что в R1 время ожидания метода истекает, и он продолжает запрашивать личность пользователя на маршрутизаторе R2. Этот процесс продолжается, пока NAS продолжает пробовать оставшиеся методы аутентификации, пока запрос пользователя не будет аутентифицирован, отклонен или завершен. Если на все методы аутентификации отвечает «Тайм-аут» (Timeout), аутентификация завершается ошибкой и соединение будет разорвано.

ПРИМЕЧАНИЕ: ответ «Отклонить» отличается от ответа «Тайм-аут». Ответ «Отклонить» указывает, что пользователь не соответствует критериям доступной базы данных идентификации и, следовательно, не проходит проверку подлинности, а запрос на доступ в Интернет отклоняется. Ответ «Тайм-аут» указывает, что сервер идентификации не может ответить на запрос идентификации. При обнаружении тайм-аута служба AAA переходит к следующему методу в списке, чтобы продолжить процесс аутентификации.

ПРИМЕЧАНИЕ: в этом документе описывается, как настроить AAA на сервере RADIUS. Подробнее о настройке сервера TACACS+ см. в разделе Настройка TACACS+.

Группа серверов AAA

Вы можете определить группу серверов AAA, включив в нее один или несколько серверов одного типа. Если на группу серверов ссылается список методов, NAS предпочтительно отправляет запросы на серверы в указанной группе серверов, когда список методов используется для реализации AAA.

Группа AAA с поддержкой VRF

Виртуальные приватные сети (VPN) позволяют пользователям безопасно распределять пропускную способность в магистральных сетях интернет-провайдеров (ISP). VPN — это набор сайтов, состоящий из общих маршрутов. Сайт STA подключается к сети интернет-провайдера через один или несколько интерфейсов. AAA поддерживает назначение таблицы VPN-маршрутизации (VRF) для каждой определяемой пользователем группы серверов.

Когда AAA реализуется сервером в группе, которой назначена таблица VRF, NAS отправляет пакеты запросов на удаленные серверы в группе серверов. Исходный IP-адрес пакетов запросов — это адрес, выбранный из таблицы VRF в соответствии с IP-адресами удаленных серверов.

Если вы запустите команду **ip radius/tacacs+ source-interface**, чтобы указать исходный интерфейс для пакетов запросов, IP-адрес, полученный из исходного интерфейса, будет иметь приоритет над исходным IP-адресом, выбранным из таблицы VRF.

1.3.1.1. Обзор

Особенность	Описание
AAA-аутентификация	Проверяет, могут ли пользователи получить доступ к Интернету
Авторизация AAA	Определяет, какими службами или разрешениями могут пользоваться пользователи
Учет AAA	Записывает использование сетевых ресурсов пользователями
Мультидоменный AAA	Создает специфичные для домена схемы AAA для станций 802.1X (STA) в разных доменах
Переключатель входа в систему для slave-устройства AAA	Предоставляет переключатель входа в систему для управления входом в систему slave-устройства AAA

Особенность	Описание
Кеширование результатов авторизации	Кеширует результаты авторизации, возвращенные с сервера, которые можно использовать для последующей авторизации на том же уровне

1.3.2. AAA-аутентификация

Аутентификация, авторизация и учет — это три независимых сервиса. Служба аутентификации проверяет, могут ли пользователи получить доступ к Интернету. Во время аутентификации между устройствами происходит обмен именем пользователя, паролем и другой информацией о пользователе для завершения доступа пользователей или запросов на обслуживание. Вы можете использовать только службу аутентификации AAA.

ПРИМЕЧАНИЕ: чтобы настроить аутентификацию AAA, необходимо сначала настроить список методов аутентификации. Приложения выполняют аутентификацию в соответствии со списком методов. Список методов определяет типы аутентификации и последовательность их выполнения. Методы аутентификации реализуются указанными приложениями. Единственным исключением является список методов по умолчанию. Все приложения используют список методов по умолчанию, если список методов не настроен.

1.3.2.1. Схема аутентификации AAA

- Нет аутентификации (**none**)

Личность доверенных пользователей не проверяется. Обычно метод без аутентификации (None) не используется.

- Локальная аутентификация (**local**)

Аутентификация выполняется на NAS, для которого настроена информация о пользователе (включая имена пользователей, пароли и пары AV). Прежде чем включить локальную аутентификацию, запустите команду **username password/secret**, чтобы создать локальную базу данных пользователей.

- Групповая аутентификация удаленного сервера (**group**)

Аутентификация выполняется совместно NAS и группой удаленных серверов через RADIUS или TACACS+. Группа серверов состоит из одного или нескольких серверов одного типа. Информация о пользователях управляется централизованно на удаленном сервере, что обеспечивает централизованную и унифицированную аутентификацию на нескольких устройствах с высокой пропускной способностью и надежностью. Вы можете настроить локальную аутентификацию в качестве резервной, чтобы избежать сбоев аутентификации, когда все серверы в группе серверов выходят из строя.

Типы аутентификации AAA

Продукты QTECH поддерживают следующие типы аутентификации:

- Аутентификация входа

Пользователи входят в интерфейс командной строки (CLI) NAS для аутентификации через Secure Shell (SSH), Telnet и протокол передачи файлов (FTP).

- Аутентификация Enable

После входа пользователей в интерфейс командной строки NAS пользователи должны пройти аутентификацию перед обновлением разрешений интерфейса командной строки. Этот процесс называется Аутентификацией Enable (в режиме Privileged EXEC).

1.3.2.2. Связанная конфигурация

Включение AAA

По умолчанию AAA отключен.

Чтобы включить AAA, запустите команду **aaa new-model**.

Настройка схемы аутентификации AAA

По умолчанию схема аутентификации AAA не настроена.

Прежде чем настраивать схему аутентификации AAA, определите, следует ли использовать локальную аутентификацию или аутентификацию удаленного сервера. Если необходимо реализовать последнее, заранее настройте сервер RADIUS или TACACS+. Если выбрана локальная аутентификация, настройте информацию о локальной базе данных пользователей на NAS.

Настройка списка методов аутентификации AAA

По умолчанию список методов аутентификации AAA не настроен.

Заранее определите режим доступа, который необходимо настроить. Затем настройте методы аутентификации в соответствии с режимом доступа.

1.3.3. Авторизация AAA

Авторизация AAA позволяет администраторам контролировать службы или разрешения пользователей. После включения авторизации AAA NAS настраивает сеансы пользователей в соответствии с файлами конфигурации пользователей, хранящимися на NAS или серверах. После авторизации пользователи могут использовать только сервисы или иметь только разрешения, разрешенные файлами конфигурации.

Схема авторизации AAA

- Прямая авторизация (**none**)

Прямая авторизация предназначена для пользователей с высоким уровнем доверия, которым назначены разрешения по умолчанию, указанные NAS.

- Локальная авторизация (**local**)

Локальная авторизация выполняется на NAS, который авторизует пользователей в соответствии с парами AV, настроенными для локальных пользователей.

- Удаленная авторизация группы серверов (**group**)

Авторизация выполняется совместно NAS и группой удаленных серверов. Вы можете настроить локальную или прямую авторизацию в качестве резервной, чтобы избежать сбоев авторизации, когда все серверы в группе серверов выходят из строя.

Типы авторизации AAA

- Авторизация EXEC

После входа пользователей в интерфейс командной строки NAS им назначаются уровни разрешений (от 0 до 15).

- Команды настройки авторизации

Пользователям назначаются разрешения на выполнение определенных команд в режимах конфигурации (включая режим глобальной конфигурации и подрежимы).

- Консольная авторизация

После того, как пользователи входят в систему через консоли, им разрешается выполнять команды.

- Командная авторизация

Авторизуйте пользователей с помощью команд после входа в интерфейс командной строки NAS.

- Сетевая авторизация

Авторизация выполняется совместно NAS и группой удаленных серверов. Вы можете настроить локальную или прямую авторизацию в режиме ожидания, чтобы избежать сбоев авторизации при сбое всех серверов в группе серверов.

1.3.3.1. Связанная конфигурация

Включение AAA

По умолчанию AAA отключен.

Чтобы включить AAA, запустите команду **aaa new-model**.

Настройка схемы авторизации AAA

По умолчанию схема авторизации AAA не настроена.

Перед настройкой схемы авторизации AAA определите, следует ли использовать локальную авторизацию или авторизацию группы серверов. Если необходимо реализовать авторизацию группы серверов, предварительно настройте сервер RADIUS или TACACS+. Если необходимо реализовать локальную авторизацию, настройте информацию о локальной базе данных пользователей на NAS.

Настройка списка методов авторизации AAA

По умолчанию список методов авторизации AAA не настроен.

Заранее определите режим доступа, который необходимо настроить. Затем настройте методы авторизации в соответствии с режимом доступа.

1.3.4. Учет AAA

AAA учет — это самостоятельный процесс того же уровня, что и аутентификация, и авторизация. В процессе учета запросы начала учета, обновления учета и завершения учета отправляются на настроенный сервер учета, который записывает использование сетевых ресурсов пользователями и выполняет учет, аудит и отслеживание действий пользователей.

В конфигурации AAA конфигурация схемы учета не является обязательной.

Схемы учета AAA

- Без учета (**none**)

Учет не ведется по пользователям.

- Местный учет (**local**)

Учет ведется на NAS, который собирает статистику и ограничивает количество локальных подключений пользователей. Биллинг не производится.

- Удаленный учет группы серверов (**group**)

Учет ведется совместно NAS и группой удаленных серверов. Вы можете настроить локальный учет как резервный, чтобы избежать сбоев учета, когда все серверы в группе серверов выходят из строя.

Типы учета AAA

- Учет EXEC

Учет выполняется, когда пользователи входят в интерфейс командной строки NAS и выходят из него.

- Учет команд

Записи хранятся по командам, которые пользователи запускают в интерфейсе командной строки NAS.

- Сетевой учет

Записи ведутся по сеансам выхода в Интернет.

1.3.4.1. Связанная конфигурация

Включение AAA

По умолчанию AAA отключен.

Чтобы включить AAA, запустите команду **aaa new-model**.

Настройка схемы учета AAA

По умолчанию метод учета AAA не настроен.

Перед настройкой схемы учета AAA определите, следует ли использовать локальный учет или удаленный учет группы серверов. Если необходимо внедрить удаленный учет группы серверов, предварительно настройте сервер RADIUS или TACACS+. Если необходимо реализовать локальный учет, настройте информацию о локальной базе данных пользователей на NAS.

Настройка списка методов учета AAA

По умолчанию список методов учета AAA не настроен.

Заранее определите режим доступа, который необходимо настроить. Затем настройте методы учета в соответствии с режимом доступа.

1.3.5. Мультидоменный AAA

В многодоменной среде NAS может предоставлять услуги AAA пользователям в разных доменах. Пользовательские AV (такие как имена пользователей и пароли, типы услуг и разрешения) могут различаться в разных доменах. Необходимо настроить домены, чтобы различать пользовательские AV в разных доменах и настроить набор AV (включая список методов службы AAA, например, RADIUS) для каждого домена.

Наши продукты поддерживают следующие форматы имени пользователя:

1. userid@domain-name (идентификатор пользователя@имя-домена).
2. domain-name\userid (имя-домена\идентификатор пользователя).
3. userid.domain-name (идентификатор пользователя.имя-домена).
4. Userid (идентификатор пользователя).

Четвертый формат (идентификатор пользователя) не содержит имя домена, и считается, что используется доменное имя по умолчанию.

NAS предоставляет услугу AAA на основе домена на основе следующих принципов:

- Разрешает доменное имя пользователя.
- Ищет домен пользователя по имени домена.
- Поиск соответствующего имени списка методов AAA в соответствии с информацией о конфигурации домена на NAS.
- Выполняет поиск соответствующего списка методов по имени списка методов.
- Предоставляет услуги AAA на основе списка методов.

ПРИМЕЧАНИЕ: если какая-либо из предыдущих процедур не удалась, услуги AAA не могут быть предоставлены.

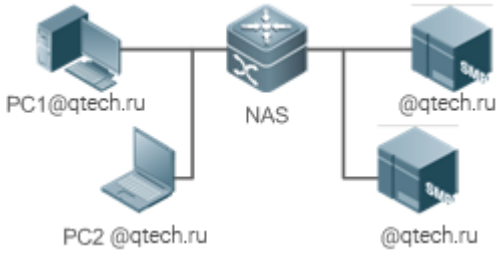


Рисунок 1-4. Типичная многодоменная топология.

1.3.5.1. Связанная конфигурация

Включение AAA

По умолчанию AAA отключен.

Чтобы включить AAA, запустите команду **aaa new-model**.

Настройка списка методов AAA

По умолчанию список методов AAA не настроен.

Включение доменной службы AAA

По умолчанию служба AAA на основе домена отключена.

Чтобы включить службу AAA на основе домена, выполните команду **aaa domain enable**.

Создание домена

По умолчанию домен не настроен.

Чтобы настроить домен, выполните команду **aaa domain** *domain-name*.

Настройка набора AV для домена

По умолчанию набор AV доменов не настроен.

Набор AV для домена содержит следующие элементы: списки методов AAA, максимальное количество онлайн-пользователей, либо удаление доменного имени из имени пользователя, либо использование доменного имени.

Отображение конфигурации домена

Чтобы отобразить конфигурацию домена, выполните команду **show aaa domain**.

ПРИМЕЧАНИЕ: система поддерживает максимум 32 домена.

1.3.6. Переключатель входа в систему для slave-устройства AAA

Переключатель входа в систему предназначен для управления входом в систему slave-устройства AAA. По умолчанию переключатель выключен, поэтому slave-устройству не разрешен вход в систему. Когда переключатель включен, slave-устройство может войти в систему.

1.3.6.1. Связанная конфигурация

Включение AAA

По умолчанию AAA отключен.

Чтобы включить AAA, запустите команду **aaa new-model**.

Настройка переключателя входа в систему для slave-устройства AAA

По умолчанию slave-устройству не разрешен вход в систему.

Запустите команду **aaa slave-login allow**, чтобы разрешить вход в систему slave-устройства.

1.3.7. Кеширование результатов авторизации

Модуль AAA кеширует результаты авторизации, возвращенные с сервера. Следовательно, более поздние авторизации на том же уровне могут выполняться на основе кешированных ресурсов.

1.3.7.1. Связанная конфигурация

Настройка кеширования результатов авторизации

По умолчанию результаты авторизации не кешируются.

Чтобы включить кеширование результатов авторизации, выполните команду **aaa command-author cache**.

Конфигурация

Конфигурация	Описание и команда	
Настройка аутентификации AAA	Обязательно, если необходимо подтвердить личность пользователя	
	aaa new-model	Включает AAA
	aaa authentication login	Определяет список методов аутентификации входа
	aaa authentication enable	Определяет список методов для включения аутентификации
	aaa authentication ppp	Определяет список методов аутентификации PPP
	aaa authentication sslvpn	Определяет список методов аутентификации SSL VPN
	login authentication	Применяет аутентификацию входа в систему к определенной завершенной строке
	aaa local authentication attempts	Устанавливает максимальное количество попыток входа в систему
	aaa local authentication lockouttime	Устанавливает время блокировки для пользователя, вошедшего в систему

Конфигурация	Описание и команда	
Настройка авторизации AAA	Обязательно, если пользователям необходимо назначить различные разрешения и службы	
	aaa new-model	Включает AAA
	aaa authorization exec	Определяет список методов авторизации EXEC
	aaa authorization commands	Определяет список методов авторизации команд
	aaa authorization network	Настраивает список методов сетевой авторизации
	authorization exec	Применяет методы авторизации EXEC к указанной строке VTY
	authorization commands	Применяет методы авторизации команд к указанной строке VTY
Настройка учета AAA	Обязательно, если необходимо вести учет, статистику и отслеживание использования сетевых ресурсов пользователями	
	aaa new-model	Включает AAA
	aaa accounting exec	Определяет список методов учета EXEC
	aaa accounting commands	Определяет список методов учета команд
	aaa accounting network	Определяет список методов сетевого учета
	accounting exec	Применяет методы учета EXEC к указанной строке VTY
	accounting commands	Применяет методы учета команд к указанной строке VTY
	aaa accounting update	Включает обновление учета

Конфигурация	Описание и команда	
Настройка учета AAA	**aaa accounting update periodic**	Настраивает интервал обновления учета
Настройка группы серверов AAA	Рекомендуется, если необходимо настроить группу серверов для обработки AAA через разные серверы в группе	
	aaa group server	Создает определяемую пользователем группу серверов AAA
	server	Добавляет члена группы серверов AAA
	ip vrf forwarding	Настраивает атрибут VRF группы серверов AAA
Настройка службы AAA на основе домена	Обязательно, если управление AAA для STA доступа 802.1X должно выполняться в соответствии с доменами	
	aaa new-model	Включает AAA
	aaa domain enable	Включает службу AAA на основе домена
	aaa domain	Создает домен и входит в режим конфигурации домена
	accounting network	Связывает домен со списком методов сетевого учета
	authorization network	Связывает домен со списком методов авторизации в сети
	state	Настраивает статус домена
	username-format	Настраивает, должно ли содержаться имя домена в именах пользователей
	access-limit	Настраивает максимальное количество пользователей домена

Конфигурация	Описание и команда	
Настройка переключателя входа в систему для slave-устройства AAA	Обязательно, если необходимо настроить переключатель входа в систему для slave-устройства AAA	
	aaa slave-login allow	Разрешает вход slave-устройства
Настройка кеширования результатов авторизации	Обязательно, если более поздние авторизации на том же уровне должны выполняться на основе прежних результатов	
	aaa command-author cache	Кеширует результаты авторизации

1.3.8. Настройка аутентификации AAA

1.3.8.1. Эффект конфигурации

Проверьте, могут ли пользователи получить разрешение на доступ.

1.3.8.2. Примечания

- Если схема аутентификации содержит несколько методов аутентификации, эти методы выполняются в соответствии с настроенной последовательностью.
- Следующий метод аутентификации выполняется только тогда, когда текущий метод не отвечает. Если текущий метод не работает, следующий метод не будет использоваться.
- Когда используется метод **none**, пользователи могут получить доступ, даже если ни один из методов идентификации не получает ответа. Поэтому метод **none** используется только в качестве резервного.

ПРИМЕЧАНИЕ: обычно не используйте проверку подлинности **none**. В особых случаях вы можете использовать метод **none** как последний необязательный метод идентификации. Например, все пользователи, которые могут запросить доступ, являются доверенными пользователями, и работа пользователей не должна задерживаться из-за системных сбоев. Затем вы можете использовать метод **none** для назначения прав доступа этим пользователям, когда сервер аутентификации не отвечает. Рекомендуется добавлять локальный метод аутентификации перед методом **none**.

- Если аутентификация AAA включена, но метод аутентификации не настроен, а метод аутентификации по умолчанию не существует, пользователи могут напрямую входить в консоль без аутентификации. Если пользователи входят в систему другими способами, они должны пройти локальную аутентификацию.
- Когда пользователь входит в интерфейс командной строки (CLI) после прохождения аутентификации при входе (метод **none** не используется), имя пользователя записывается. Когда пользователь выполняет Аутентификацию включения, пользователю не предлагается снова ввести имя пользователя, потому что имя пользователя, которое пользователь ввел во время аутентификации при входе, заполняется автоматически. Однако пользователь должен ввести пароль, ранее использовавшийся для аутентификации при входе.
- Имя пользователя не записывается, если пользователь не выполняет аутентификацию при входе в CLI или во время аутентификации при входе

используется метод **none**. Поэтому пользователь должен вводить имя пользователя каждый раз при выполнении идентификации.

1.3.8.3. Шаги настройки

Включение AAA

- Обязательный.
- Запустите команду **aaa new-model**, чтобы включить AAA.
- По умолчанию AAA отключен.

Определение списка методов аутентификации при входе

- Запустите команду **aaa authentication login**, чтобы настроить список методов аутентификации входа.
- Эта конфигурация является обязательной, если вам необходимо настроить список методов аутентификации при входе (включая конфигурацию списка методов по умолчанию).
- По умолчанию список методов аутентификации при входе не настроен.

Определение списка методов для включения аутентификации

- Запустите команду **aaa authentication enable**, чтобы настроить список методов для включения аутентификации.
- Эта конфигурация является обязательной, если вам нужно настроить список методов аутентификации. (Можно настроить только список методов по умолчанию.)
- По умолчанию список методов для включения аутентификации не настроен.

Определение списка методов аутентификации PPP

- Запустите команду **aaa authentication ppp**, чтобы настроить список методов аутентификации PPP.
- Эта конфигурация обязательна, если вам нужно настроить список методов аутентификации для коммутируемого доступа PPP.
- По умолчанию список методов аутентификации PPP не настроен.

Определение списка методов аутентификации SSL VPN

- Запустите команду **aaa authentication sslvpn**, чтобы настроить список методов аутентификации SSL VPN.
- Эта конфигурация обязательна, если вам нужно настроить список методов аутентификации SSL VPN (включая конфигурацию списка методов по умолчанию).
- По умолчанию список методов аутентификации SSL VPN не настроен.

Применение аутентификации при входе в систему к определенной завершенной строке

- В режиме конфигурации запустите команду **login authentication**, чтобы применить аутентификацию входа к определенной завершенной строке.
- Эта конфигурация обязательна, если вам нужно применить аутентификацию входа в систему к определенной завершенной строке.
- По умолчанию список методов по умолчанию применяется ко всем завершенным строкам.

Установка максимального количества попыток входа в систему

- Опционально.

- По умолчанию пользователю разрешено вводить пароли до трех раз при входе в систему.

Установка максимального времени блокировки после сбоя входа в систему

- Опционально.
- По умолчанию пользователь блокируется на 15 минут после трехкратного ввода неверного пароля.

1.3.8.4. Проверка

- Запустите команду **show aaa method-list**, чтобы отобразить настроенные списки методов.
- Запустите команду **show aaa lockout**, чтобы отобразить настройки максимального количества попыток входа и максимального времени блокировки после неудачного входа.
- Запустите команду **show running-config**, чтобы отобразить списки методов аутентификации, связанные с аутентификацией при входе в систему.

1.3.8.5. Связанные команды

Включение AAA

Команда	**aaa new-model**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы включить службы AAA, выполните эту команду. Ни одна из остальных команд AAA не может быть эффективной, если AAA не включена

Определение списка методов аутентификации при входе

Команда	**aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]
Описание параметров	**default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает название списка методов аутентификации при входе в систему в виде символов. *method*: указывает методы аутентификации: local, none или group. Список методов содержит до четырех методов. local: указывает, что для аутентификации используется локальная база данных пользователей. none: указывает, что аутентификация не выполняется. group: указывает, что группа серверов используется для аутентификации. В настоящее время поддерживаются группы серверов RADIUS и TACACS+

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если на NAS включена служба аутентификации входа AAA, пользователи должны выполнять согласование аутентификации входа через AAA. Запустите команду аутентификации входа в систему, чтобы настроить списки методов по умолчанию или необязательные для аутентификации при входе. В списке методов следующий метод выполняется только тогда, когда текущий метод не получает ответа. После настройки методов аутентификации при входе в систему примените эти методы к строкам VTY, требующим аутентификации при входе; в противном случае методы не подействуют

Определение списка методов для включения аутентификации

Команда	**aaa authentication enable default** *method1* [*method2*...]
Описание параметров	**default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *method*: указывает методы аутентификации: local, none или group. Список методов содержит до четырех методов. enable: указывает, что пароль, настроенный с помощью команды enable, используется для аутентификации. local: указывает, что для аутентификации используется локальная база данных пользователей. none: указывает, что аутентификация не выполняется. group: указывает, что группа серверов используется для идентификации. В настоящее время поддерживаются группы серверов RADIUS и TACACS+
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если на NAS включена служба аутентификации входа AAA, пользователи должны выполнить согласование аутентификации с помощью AAA. Запустите команду включения аутентификации AAA, чтобы настроить списки методов по умолчанию или дополнительные методы для включения аутентификации. В списке методов следующий метод выполняется только тогда, когда текущий метод не получает ответа

Определение списка методов аутентификации PPP, Web, iPortal или SSL VPN

Команда	**aaa authentication** { **ppp** | **sslvpn** } { **default** | *list-name* } *method1* [*method2*...]
Описание параметров	**ppp**: настраивает список методов аутентификации PPP. **sslvpn**: настраивает список методов аутентификации SSL VPN. **default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает имя списка методов аутентификации PPP в символах. *method*: указывает методы аутентификации: local, none, group или subs. Список методов содержит до четырех методов. local: указывает, что для аутентификации используется локальная база данных пользователей. none: указывает, что аутентификация не выполняется. group: указывает, что группа серверов используется для идентификации. В настоящее время поддерживаются группы серверов RADIUS и TACACS+. subs: указывает метод аутентификации SUBS с использованием базы данных SUBS
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если на NAS включена служба аутентификации AAA PPP, пользователи должны выполнять согласование аутентификации PPP через AAA. Запустите команду аутентификации AAA PPP, чтобы настроить списки методов по умолчанию или дополнительные методы для аутентификации PPP. В списке методов следующий метод выполняется только тогда, когда текущий метод не получает ответа

Установка максимального количества попыток входа в систему

Команда	**aaa local authentication attempts** *max-attempts*
Описание параметров	*max-attempts*: указывает максимальное количество попыток входа в систему. Значение находится в диапазоне от 1 до 2 147 483 647
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы установить максимальное количество попыток входа пользователя в систему

Установка максимального времени блокировки после сбоя входа в систему

Команда	**aaa local authentication lockout-time** *lockout-time*
Описание параметров	*lockout-time*: указывает время, в течение которого пользователь заблокирован после ввода неправильных паролей до указанного количества раз. Значение варьируется от 1 до 2 147 483 647, в минутах
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы установить максимальное время, в течение которого пользователь будет заблокирован после ввода неправильного пароля до указанного количества раз

1.3.8.6. Пример конфигурации

Настройка аутентификации входа AAA

Настройте список методов аутентификации при входе на NAS, содержащий **group** *radius* и **local** методы по порядку.

Сценарий:



Рисунок 1-5.

Шаги настройки	**Шаг 1.** Включите AAA. **Шаг 2.** Заранее настройте сервер RADIUS или TACACS+, если необходимо реализовать аутентификацию группы серверов. Настройте информацию о локальной базе данных пользователей на NAS, если необходимо реализовать локальную аутентификацию. (В этом примере требуется настройка сервера RADIUS и информации о локальной базе данных.) **Шаг 3.** Настройте список методов аутентификации AAA для пользователей аутентификации при входе в систему. (В этом примере используется **group** *radius* и **local** по порядку.) **Шаг 4.** Примените настроенный список методов к интерфейсу или строке. Пропустите этот шаг, если используется метод аутентификации по умолчанию
NAS	QTECH#configure terminal QTECH(config)#username user password pass QTECH(config)#aaa new-model

	QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key QTECH QTECH(config)#aaa authentication login list1 group radius local QTECH(config)#line vty 0 20 QTECH(config-line)#login authentication list1 QTECH(config-line)#exit
Проверка	Запустите команду **show aaa method-list** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa method-list Authentication method-list: aaa authentication login list1 group radius local Accounting method-list: Authorization method-list:
	Предположим, что пользователь удаленно входит в NAS через Telnet. Пользователю предлагается ввести имя пользователя и пароль в интерфейсе командной строки. Пользователь должен ввести правильное имя пользователя и пароль для доступа к NAS
Пользо-ватель	User Access Verification Username:user Password:pass

Настройка Аутентификации Enable AAA

Настройте список методов Аутентификации Enable на NAS, содержащий **group** *radius*, **local** и **enable** методы по порядку.

Сценарий:



Рисунок 1-6.

Шаги настройки	**Шаг 1.** Включите AAA. **Шаг 2.** Заранее настройте сервер RADIUS или TACACS+, если необходимо реализовать групповую аутентификацию на сервере. Настройте информацию о локальной базе данных пользователей на NAS, если необходимо реализовать локальную аутентификацию. Настройте пароли Аутентификации Enable на NAS, если вы используете пароль для Аутентификации Enable. **Шаг 3.** Настройте список методов аутентификации AAA для пользователей Аутентификации Enable. **ПРИМЕЧАНИЕ:** вы можете определить глобально только один список методов Аутентификации Enable. Вам не нужно определять имя списка, а просто использовать его по умолчанию. После этого он будет применяться автоматически
NAS	QTECH#configure terminal QTECH(config)#username user privilege 15 password pass QTECH(config)#enable secret w QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key QTECH QTECH(config)#aaa authentication enable default group radius local enable
Проверка	Запустите команду **show aaa method-list** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa method-list Authentication method-list: aaa authentication enable default group radius local enable Accounting method-list: Authorization method-list:
	Интерфейс командной строки отображает запрос на аутентификацию, когда уровень пользователя обновляется до уровня 15. Пользователь должен ввести правильное имя пользователя и пароль для доступа к NAS
NAS	QTECH>enable Username:user Password:pass

	QTECH#

1.3.8.7. Распространенные ошибки

- Сервер RADIUS или сервер TACACS+ не настроены.
- Имена пользователей и пароли не настроены в локальной базе данных.

1.3.9. Настройка авторизации AAA

1.3.9.1. Эффект конфигурации

Определите, какими службами или разрешениями могут пользоваться пользователи, прошедшие аутентификацию.

1.3.9.2. Примечания

- Авторизация EXEC часто используется с аутентификацией при входе в систему, которая может быть реализована в одной строке. Авторизация и аутентификация могут выполняться с использованием различных методов и серверов. Поэтому результаты одного и того же пользователя могут быть разными. Если пользователь проходит аутентификацию при входе в систему, но не проходит авторизацию EXEC, пользователь не может войти в интерфейс командной строки.
- Методы авторизации в схеме авторизации выполняются в соответствии с последовательностью конфигурации метода. Следующий метод авторизации выполняется только тогда, когда текущий метод не получает ответа. Если авторизация не удалась с помощью метода, следующий метод не будет использоваться.
- Авторизация команд поддерживается только TACACS+.
- Авторизация через консоль: ПО может различать пользователей, которые входят в систему через консоль, и пользователей, которые входят в систему через другие типы клиентов. Вы можете включить или отключить авторизацию команд для пользователей, которые входят в систему через консоль. Если для этих пользователей отключена авторизация команд, то список методов авторизации команд, примененный к строке консоли, больше не действует.

1.3.9.3. Шаги настройки

Включение AAA

- Обязательный.
- Запустите команду **aaa new-model**, чтобы включить AAA.
- По умолчанию AAA отключен.

Определение списка методов авторизации EXEC

- Запустите команду **aaa authorization exec**, чтобы настроить список методов авторизации EXEC.
- Эта конфигурация обязательна, если вам нужно настроить список методов авторизации EXEC (включая настройку списка методов по умолчанию).
- По умолчанию список методов авторизации EXEC не настроен.

ПРИМЕЧАНИЕ: уровень разрешений доступа по умолчанию для пользователей EXEC — самый низкий. (Пользователи консоли могут подключаться к NAS через консольный порт или через Telnet. Каждое подключение считается пользователем EXEC, например, пользователем Telnet и пользователем SSH.)

Определение списка методов авторизации команд

- Запустите команду **aaa authorization commands**, чтобы настроить список методов авторизации команд.
- Эта конфигурация обязательна, если вам нужно настроить список методов авторизации команд (включая настройку списка методов по умолчанию).
- По умолчанию список методов авторизации команд не настроен.

Настройка списка методов сетевой авторизации

- Запустите команду **aaa authorization network**, чтобы настроить список методов сетевой авторизации.
- Эта конфигурация обязательна, если вам нужно настроить список методов сетевой авторизации (включая настройку списка методов по умолчанию).
- По умолчанию метод авторизации не настроен.

Применение методов авторизации EXEC к указанной строке VTY

- Запустите команду **authorization exec** в режиме конфигурации строки, чтобы применить методы авторизации EXEC к указанной строке VTY.
- Эта конфигурация обязательна, если вам нужно применить список методов авторизации EXEC к указанной строке VTY.
- По умолчанию все строки VTY связаны со списком методов авторизации по умолчанию.

Применение методов авторизации команд к указанной строке VTY

- Запустите команду **authorization commands** в режиме конфигурации строки чтобы применить методы авторизации команд к указанной строке VTY.
- Эта конфигурация является обязательной, если вам нужно применить список методов авторизации команд к указанной строке VTY.
- По умолчанию все строки VTY связаны со списком методов авторизации по умолчанию.

Включение авторизации для команд в режимах конфигурации

- Запустите команду **aaa authorization config-commands**, чтобы включить авторизацию для команд в режимах конфигурации.
- По умолчанию авторизация отключена для команд в режимах конфигурации.

Включение авторизации для консоли для выполнения команд

- Запустите команду **aaa authorization console**, чтобы включить авторизацию для пользователей консоли для выполнения команд.
- По умолчанию авторизация отключена для консоли для запуска команд.

1.3.9.4. Проверка

Запустите команду **show running-config**, чтобы проверить конфигурацию.

1.3.9.5. Связанные команды

Включение AAA

Команда	**aaa new-model**
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Чтобы включить службы AAA, выполните эту команду. Ни одна из остальных команд AAA не может быть эффективной, если AAA не включена

Определение списка методов авторизации EXEC

Команда	**aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]
Описание параметров	**default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает имя списка методов авторизации EXEC в символах. *method*: указывает методы аутентификации: local, none и group. Список методов содержит до четырех методов. local: указывает, что локальная база данных пользователей используется для авторизации EXEC. none: указывает, что авторизация EXEC не выполняется. group: указывает, что для авторизации EXEC используется группа серверов. В настоящее время поддерживаются группы серверов RADIUS и TACACS+
Командный режим	Режим глобальной конфигурации
Руководство по использованию	ПО поддерживает авторизацию пользователей, которые входят в интерфейс командной строки NAS, для назначения уровней разрешений на операции с интерфейсом пользователя (от 0 до 15). В настоящее время авторизация EXEC выполняется только для пользователей, прошедших аутентификацию при входе в систему. Если пользователю не удается выполнить авторизацию EXEC, он не может войти в интерфейс командной строки. После настройки методов авторизации EXEC примените методы к строкам VTY, для которых требуется авторизация EXEC; в противном случае методы не подействуют

Определение списка методов авторизации команд

Команда	**aaa authorization commands level** { **default** | *list-name* } *method1* [*method2*...]
Описание параметров	**default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает имя списка методов авторизации команд в символах. *method*: указывает методы аутентификации из none и group. Список методов содержит до четырех методов.

	none: указывает, что авторизация команды не выполняется. group: указывает, что для авторизации команд используется группа серверов. В настоящее время поддерживается группа серверов TACACS+
Командный режим	Режим глобальной конфигурации
Руководство по использованию	ПО поддерживает авторизацию команд, выполняемых пользователями. Когда пользователь вводит команду, AAA отправляет команду на сервер аутентификации. Если сервер аутентификации разрешает выполнение, команда выполняется. Если сервер аутентификации запрещает выполнение, команда не выполняется и отображается сообщение о том, что выполнение отклонено. При настройке авторизации команд укажите уровень команды, который используется в качестве уровня по умолчанию. (Например, если команда уровня выше 14 видна пользователям, уровень команды по умолчанию — 14.) После настройки методов авторизации команд примените эти методы к строкам VTY, требующим авторизации команд; в противном случае методы не подействуют

Настройка списка методов сетевой авторизации

Команда	**aaa authorization network** { **default** | *list-name* } *method1* [*method2*...]
Описание параметров	**default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает имя списка методов авторизации в сети в символах. *method*: указывает методы аутентификации из none и group. Список методов содержит до четырех методов. none: указывает, что аутентификация не выполняется. group: указывает, что для авторизации в сети используется группа серверов. В настоящее время поддерживаются группы серверов RADIUS и TACACS+
Командный режим	Режим глобальной конфигурации

Руководство по использованию	ПО поддерживает авторизацию сетевых сервисных запросов, таких как запросы PPP и SLIP. После настройки авторизации все аутентифицированные пользователи или интерфейсы авторизуются автоматически. Вы можете настроить три различных метода авторизации. Следующий метод авторизации выполняется только тогда, когда текущий метод не получает ответа. Если авторизация не удалась с помощью метода, следующий метод не будет использоваться. Серверы RADIUS или TACACS+ возвращают серию пар AV для авторизации аутентифицированных пользователей. Авторизация в сети основана на аутентификации. Только аутентифицированные пользователи могут выполнять сетевую авторизацию

Включение авторизации для команд в режимах конфигурации (включая режим глобальной конфигурации и подрежимы)

Команда	**aaa authorization config-commands**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если вам нужно включить авторизацию для команд только в неконфигурационных режимах (например, в привилегированном режиме EXEC), отключите авторизацию в конфигурационных режимах, используя форму no этой команды. Затем пользователи могут запускать команды в режиме конфигурации и подрежимах без авторизации

Включение авторизации для консоли для выполнения команд

Команда	**aaa authorization console**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	ПО может различать пользователей, которые входят в систему через консоль и пользователей, которые входят в систему через другие типы клиентов. Вы можете включить или отключить авторизацию команд для пользователей, которые входят в систему через консоль. Если авторизация команд отключена для этих пользователей, список методов авторизации команд, примененный к строке консоли, больше не вступает в силу

1.3.9.6. Пример конфигурации

Настройка авторизации AAA EXEC

Настройка аутентификации входа и авторизация EXEC для пользователей на строках VTY с 0 по 4. Аутентификация входа выполняется в локальном режиме, а авторизация EXEC

выполняется на сервере RADIUS. Если сервер RADIUS не отвечает, пользователи перенаправляются на локальную авторизацию.

Сценарий:



Рисунок 1-7.

Шаги настройки	**Шаг 1.** Включите AAA. **Шаг 2.** Заранее настройте сервер RADIUS или TACACS+, если необходимо реализовать удаленную авторизацию группы серверов. Если необходимо реализовать локальную авторизацию, настройте информацию о локальной базе данных пользователей на NAS. **Шаг 3.** Настройте список методов авторизации AAA в соответствии с различными режимами доступа и типами услуг. **Шаг 4.** Примените настроенный список методов к интерфейсу или линии. Пропустите этот шаг, если используется метод авторизации по умолчанию. Авторизация EXEC часто используется с аутентификацией при входе в систему, которая может быть реализована в одной строке
NAS	QTECH#configure terminal QTECH(config)#username user password pass QTECH(config)#username user privilege 6 QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key test QTECH(config)#aaa authentication login list1 group local QTECH(config)#aaa authorization exec list2 group radius local QTECH(config)#line vty 0 4 QTECH(config-line)#login authentication list1 QTECH(config-line)# authorization exec list2 QTECH(config-line)#exit
Проверка	Запустите команды **show run** и **show aaa method-list** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa method-list Authentication method-list:

	aaa authentication login list1 group local Accounting method-list: Authorization method-list: aaa authorization exec list2 group radius local
	QTECH# show running-config aaa new-model ! aaa authorization exec list2 group local aaa authentication login list1 group radius local ! username user password pass username user privilege 6 ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4 authorization exec list2 login authentication list1 ! End

Настройка авторизации команд AAA

Обеспечьте авторизацию команд для зарегистрированных пользователей в соответствии со следующим методом авторизации по умолчанию: Сначала авторизуйте команды уровня 15 с помощью сервера TACACS+. Если сервер TACACS+ не отвечает, выполняется локальная авторизация. Авторизация применяется к пользователям, которые входят в систему через консоль, и пользователям, которые входят в систему через другие типы клиентов.

Сценарий:



Рисунок 1-8.

Шаги настройки	**Шаг 1.** Включите AAA. **Шаг 2.** Заранее настройте сервер RADIUS или TACACS+, если необходимо реализовать удаленную авторизацию группы серверов. Если необходимо реализовать локальную авторизацию, настройте информацию о локальной базе данных пользователей на NAS. **Шаг 3.** Настройте список методов авторизации AAA в соответствии с различными режимами доступа и типами услуг. **Шаг 4.** Примените настроенный список методов к интерфейсу или линии. Пропустите этот шаг, если используется метод авторизации по умолчанию
NAS	QTECH#configure terminal QTECH(config)#username user1 password pass1 QTECH(config)#username user1 privilege 15 QTECH(config)#aaa new-model QTECH(config)#tacacs-server host 192.168.217.10 QTECH(config)#tacacs-server key aaa QTECH(config)#aaa authentication login default local QTECH(config)#aaa authorization commands 15 default group tacacs+ local QTECH(config)#aaa authorization console
Проверка	Запустите команды **show run** и **show aaa method-list** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: Authorization method-list: aaa authorization commands 15 default group tacacs+ local
	QTECH#show run ! aaa new-model ! aaa authorization console aaa authorization commands 15 default group tacacs+ local

	aaa authentication login default local ! ! nfpp ! vlan 1 ! username user1 password 0 pass1 username user1 privilege 15 no service password-encryption ! tacacs-server host 192.168.217.10 tacacs-server key aaa ! line con 0 line vty 0 4 ! ! end

Настройка сетевой авторизации AAA

Сценарий:



Рисунок 1-9.

Шаги настройки	**Шаг 1.** Включите AAA. **Шаг 2.** Заранее настройте сервер RADIUS или TACACS+, если необходимо реализовать удаленную авторизацию группы серверов. Если необходимо реализовать локальную авторизацию, настройте информацию о локальной базе данных пользователей на NAS. **Шаг 3.** Настройте список методов авторизации AAA в соответствии с различными режимами доступа и типами услуг. **Шаг 4.** Примените настроенный список методов к интерфейсу или линии. Пропустите этот шаг, если используется метод авторизации по умолчанию
NAS	QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1

	QTECH(config)#radius-server key test QTECH(config)#aaa authorization network default group radius none QTECH(config)# end
Проверка	Запустите команду **show aaa method-list** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa method-list Authentication method-list: Accounting method-list: Authorization method-list: aaa authorization network default group radius none

1.3.10. Настройка учета AAA

1.3.10.1. Эффект конфигурации

- Записывает использование сетевых ресурсов пользователями.
- Записывает процессы входа и выхода пользователей, а также команды, выполняемые пользователями во время управления устройством.

1.3.10.2. Примечания

О методах учета

- Если схема учета содержит несколько методов учета, эти методы выполняются в соответствии с последовательностью настройки методов. Следующий метод учета выполняется только тогда, когда текущий метод не получает ответа. Если учет не работает с использованием метода, следующий метод не будет использоваться.
- После настройки списка методов учета по умолчанию он автоматически применяется ко всем строкам VTY. Если к строке применяется список методов учета не по умолчанию, он заменит список по умолчанию. Если вы примените неопределенный список методов к строке, система выдаст сообщение о том, что учет в этой строке неэффективен. Учет вступит в силу только тогда, когда будет применен определенный список методов.

Учет EXEC

Учет EXEC выполняется только после завершения аутентификации при входе в NAS. Учет EXEC не выполняется, если аутентификация при входе не настроена или для аутентификации используется метод **none**. Если «Начало» учета не выполняется для пользователя при входе в систему, «Конец» учета не будет выполняться при выходе пользователя из системы.

Учет команд

Только протокол TACACS+ поддерживает учет команд.

1.3.10.3. Шаги настройки

Включение AAA

- Обязательный.
- Запустите команду **aaa new-model**, чтобы включить AAA.
- По умолчанию AAA отключен.

Определение списка методов учёта EXEC

- Запустите команду **aaa accounting exec** для настройки списка методов учета EXEC.
- Эта конфигурация обязательна, если вам нужно настроить список методов учета EXEC (включая настройку списка методов по умолчанию).
- Уровень разрешений доступа по умолчанию для пользователей EXEC — самый низкий. (Пользователи консоли могут подключаться к NAS через консольный порт или через Telnet. Каждое подключение считается пользователем EXEC, например, пользователем Telnet и пользователем SSH.)
- По умолчанию список методов учета EXEC не настроен.

Определение списка методов учета команд

- Запустите команду **aaa accounting commands**, чтобы настроить список методов учета команд.
- Эта конфигурация обязательна, если вам нужно настроить список методов учета команд (включая настройку списка методов по умолчанию).
- По умолчанию список методов учета команд не настроен. Только протокол TACACS+ поддерживает учет команд.

Определение списка методов сетевого учета

- Запустите команду **aaa accounting network**, чтобы настроить список методов учета сети.
- Эта конфигурация обязательна, если вам нужно настроить список методов сетевого учета (включая настройку списка методов по умолчанию).
- По умолчанию список методов сетевого учета не настроен.

Применение методов учета EXEC к указанной строке VTY

- Запустите команду **accounting exec** в режиме конфигурации строки, чтобы применить методы учета EXEC к указанной строке VTY.
- Эта конфигурация является обязательной, если вам нужно применить список методов учета EXEC к указанной строке VTY.
- Вам не нужно запускать эту команду, если вы применяете список методов по умолчанию.
- По умолчанию все строки VTY связаны со списком методов учета по умолчанию.

Применение методов учета команд к указанной строке VTY

- Запустите команду **accounting commands** в режиме конфигурации строки, чтобы применить методы учета команд к указанной строке VTY.
- Эта конфигурация обязательна, если вам нужно применить список методов учета команд к указанной строке VTY.
- Вам не нужно запускать эту команду, если вы применяете список методов по умолчанию.
- По умолчанию все строки VTY связаны со списком методов учета по умолчанию.

Включение обновления учета

- Опционально.
- Рекомендуется настроить обновление учета для повышения точности учета.
- По умолчанию обновление учета отключено.

Настройка интервала обновления учета

- Опционально.
- Рекомендуется не настраивать интервал обновления учета, если не указано иное.

1.3.10.4. Проверка

Запустите команду **show running-config**, чтобы проверить конфигурацию.

1.3.10.5. Связанные команды

Включение AAA

Команда	**aaa new-model**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы включить службы AAA, выполните эту команду. Ни одна из остальных команд AAA не может быть эффективной, если AAA не включена

Определение списка методов учёта EXEC

Команда	**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Описание параметров	**default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает имя списка методов учета EXEC в символах. *method*: указывает методы идентификации из none и group. Список методов содержит до четырех методов. none: указывает, что учет EXEC не выполняется. group: указывает, что группа серверов используется для учета EXEC. В настоящее время поддерживаются группы серверов RADIUS и TACACS+
Командный режим	Режим глобальной конфигурации
Руководство по использованию	ПО включает учет EXEC только после завершения аутентификации при входе. Учет EXEC не выполняется, если не выполняется аутентификация при входе в систему или используется метод без аутентификации.

	После включения учета, когда пользователь входит в интерфейс командной строки NAS, NAS отправляет сообщение запуска учета на сервер аутентификации. Когда пользователь выходит из системы, NAS отправляет сообщение об остановке учета на сервер аутентификации. Если NAS не отправляет сообщение о начале учета при входе пользователя в систему, NAS не будет отправлять сообщение об остановке учета при выходе пользователя из системы. После настройки методов учета EXEC примените методы к строкам VTY, требующим учета EXEC; в противном случае методы не подействуют

Определение списка методов учета команд

Команда	**aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Описание параметров	*level*: указывает уровень команды, для которого будет выполняться учет. Значение находится в диапазоне от 0 до 15. После выполнения команды сконфигурированного уровня учетный сервер записывает соответствующую информацию на основе полученного учетного пакета. **default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает имя списка методов учета команд в символах. *method*: указывает методы идентификации из none and group. Список методов содержит до четырех методов. none: указывает, что учет команд не выполняется. group: указывает, что группа серверов используется для учета команд. В настоящее время поддерживается группа серверов TACACS+
Командный режим	Режим глобальной конфигурации
Руководство по использованию	ПО включает учет команд только после завершения аутентификации при входе в систему. Учет команд не выполняется, если не выполняется аутентификация при входе в систему или используется метод без аутентификации. После включения учета NAS записывает информацию о командах настроенного уровня, которые запускают пользователи, и отправляет информацию на сервер аутентификации. После настройки методов учета команд примените методы к строкам VTY, требующим учета команд; в противном случае методы не подействуют

Определение списка методов сетевого учета

Команда	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Описание параметров	**default**: при использовании этого параметра сконфигурированный список методов будет использоваться по умолчанию. *list-name*: указывает имя списка методов сетевого учета в символах. **start-stop**: указывает, что сообщение начала учета и сообщение остановки учета отправляются, когда пользователь получает доступ к сети и когда пользователь отключается от сети соответственно. Сообщение «Начала» учета указывает, что пользователю разрешен доступ к сети, независимо от того, успешно ли включен учет. *method*: указывает методы идентификации из none и group. Список методов содержит до четырех методов. none: указывает, что сетевой учет не выполняется. group: указывает, что группа серверов используется для сетевого учета. В настоящее время поддерживаются группы серверов RADIUS и TACACS+
Командный режим	Режим глобальной конфигурации
Руководство по использованию	ПО отправляет атрибуты записи на сервер аутентификации для учета действий пользователя. Ключевое слово **start-stop** используется для настройки параметров учета пользователей

Включение обновления учета

Команда	**aaa accounting update**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Обновление учета нельзя использовать, если службы AAA не включены. После включения служб AAA, запустите эту команду, чтобы включить обновление учета

Настройка интервала обновления учета

Команда	**aaa accounting update periodic** *interval*
Описание параметров	*interval*: указывает интервал обновления учета в минутах. Самый короткий — 1 минута
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Обновление учета нельзя использовать, если службы AAA не включены. После включения служб AAA, запустите эту команду, чтобы настроить интервал обновления учета

1.3.10.6. Пример конфигурации

Настройка учета AAA EXEC

Настройте аутентификацию при входе и учет EXEC для пользователей на строках VTY с 0 по 4. Аутентификация при входе выполняется в локальном режиме, а учет EXEC выполняется на сервере RADIUS.

Сценарий:



Рисунок 1-10.

Шаги настройки	**Шаг 1.** Включите AAA. Если необходимо реализовать удаленный учет группы серверов, заранее настройте сервер RADIUS или TACACS+. **Шаг 2.** Настройте список методов учета AAA в соответствии с различными режимами доступа и типами услуг. **Шаг 3.** Примените настроенный список методов к интерфейсу или строке. Пропустите этот шаг, если используется метод учета по умолчанию
NAS	QTECH#configure terminal QTECH(config)#username user password pass QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key test QTECH(config)#aaa authentication login list1 group local QTECH(config)#aaa accounting exec list3 start-stop group radius QTECH(config)#line vty 0 4 QTECH(config-line)#login authentication list1 QTECH(config-line)# accounting exec list3 QTECH(config-line)#exit
Проверка	Запустите команды **show run** и **show aaa method-list** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa method-list

	Authentication method-list: aaa authentication login list1 group local Accounting method-list: aaa accounting exec list3 start-stop group radius Authorization method-list:
	QTECH# show running-config aaa new-model ! aaa accounting exec list3 start-stop group radius aaa authentication login list1 group local ! username user password pass ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4 accounting exec list3 login authentication list1 ! End

Настройка учета команд AAA

Настройте учет команд для пользователей, вошедших в систему, в соответствии с методом учета по умолчанию. Аутентификация при входе выполняется в локальном режиме, а учет команд выполняется на сервере TACACS+.

Сценарий:



Рисунок 1-11.

Шаги настройки	**Шаг 1.** Включите AAA. Если необходимо реализовать удаленный учет группы серверов, заранее настройте сервер RADIUS или TACACS+. **Шаг 2.** Настройте список методов учета AAA в соответствии с различными режимами доступа и типами услуг. **Шаг 3.** Примените настроенный список методов к интерфейсу или строке. Пропустите этот шаг, если используется метод учета по умолчанию
NAS	QTECH#configure terminal QTECH(config)#username user1 password pass1 QTECH(config)#username user1 privilege 15 QTECH(config)#aaa new-model QTECH(config)#tacacs-server host 192.168.217.10 QTECH(config)#tacacs-server key aaa QTECH(config)#aaa authentication login default local QTECH(config)#aaa accounting commands 15 default start-stop group tacacs+
Проверка	Запустите команду **show aaa method-list** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: aaa accounting commands 15 default start-stop group tacacs+ Authorization method-list:
	QTECH#show run ! aaa new-model ! aaa authorization config-commands aaa accounting commands 15 default start-stop group tacacs+ aaa authentication login default local ! ! nfpp !

```
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
! !
end
```

1.3.11. Настройка группы серверов AAA

1.3.11.1. Эффект конфигурации

- Создайте определяемую пользователем группу серверов и добавьте в группу один или несколько серверов.
- При настройке списков методов идентификации, авторизации и учета назовите методы после имени группы серверов, чтобы серверы в группе использовались для обработки запросов идентификации, авторизации и учета.
- Используйте самоопределяемые группы серверов для разделения аутентификации, авторизации и учета.

1.3.11.2. Примечания

В определяемой пользователем группе серверов можно указать и применить только серверы из группы серверов по умолчанию.

1.3.11.3. Шаги настройки

Создание определяемой пользователем группы серверов AAA

- Обязательный.
- Назначьте осмысленное имя пользовательской группе серверов. Не используйте предопределенные ключевые слова **radius** и **tacacs+** в именовании.

Добавление члена группы серверов AAA

- Обязательный.
- Запустите команду **server**, чтобы добавить членов группы серверов AAA.
- По умолчанию пользовательская группа серверов не имеет серверов.

Настройка атрибута VRF группы серверов AAA

- Необязательный.
- Запустите команду **ip vrf forwarding**, чтобы настроить атрибут VRF группы серверов AAA.

- По умолчанию группа серверов AAA принадлежит глобальной таблице VRF.

1.3.11.4. Проверка

Запустите команду **show aaa group**, чтобы проверить конфигурацию.

1.3.11.5. Связанные команды

Создание определяемой пользователем группы серверов AAA

Команда	**aaa group server** {**radius** | **tacacs+**} *name*
Описание параметров	*name*: указывает имя создаваемой группы серверов. Имя не должно содержать ключевые слова **radius** и **tacacs+**, поскольку они являются именами групп серверов RADIUS и TACACS+ по умолчанию
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для настройки группы серверов AAA. В настоящее время поддерживаются группы серверов RADIUS и TACACS+

Добавление члена группы серверов AAA

Команда	**server** *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]
Описание параметров	*ip-addr*: указывает IP-адрес сервера. *port1*: указывает порт аутентификации сервера. (Этот параметр поддерживается только группой серверов RADIUS.) *port2*: указывает порт учета сервера. (Этот параметр поддерживается только группой серверов RADIUS.)
Командный режим	Режим конфигурации группы серверов
Руководство по использованию	Когда вы добавляете серверы в группу серверов, используются порты по умолчанию, если вы не укажете порты

Настройка атрибута VRF группы серверов AAA

Команда	**ip vrf forwarding** *vrf_name*
Описание параметров	*vrf_name*: указывает имя таблицы VRF
Командный режим	Режим конфигурации группы серверов

Руководство по использованию	Используйте эту команду, чтобы назначить таблицу VRF указанной группе серверов

1.3.11.6. Пример конфигурации

Создание группы серверов AAA

Создайте группы серверов RADIUS с именами g1 и g2. IP-адреса серверов в g1 — 10.1.1.1 и 10.1.1.2, а IP-адреса серверов в g2 — 10.1.1.3 и 10.1.1.4.

Сценарий:

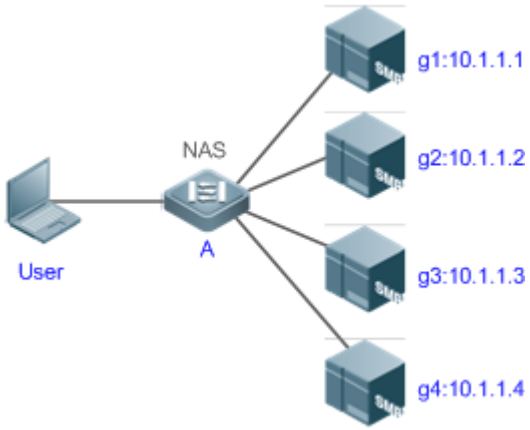


Рисунок 1-12.

Предпосылки	1. В сети настроены необходимые интерфейсы, IP-адреса и VLAN, настроены сетевые подключения и доступны маршруты от NAS к серверам. 2. Включено AAA
Шаги настройки	**Шаг 1.** Настройте сервер (который принадлежит к группе серверов по умолчанию). **Шаг 2.** Создайте определяемые пользователем группы серверов AAA. **Шаг 3.** Добавьте серверы в группы серверов AAA
NAS	QTECH#configure terminal QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server host 10.1.1.2 QTECH(config)#radius-server host 10.1.1.3 QTECH(config)#radius-server host 10.1.1.4 QTECH(config)#radius-server key secret QTECH(config)#aaa group server radius g1 QTECH(config-gs-radius)#server 10.1.1.1 QTECH(config-gs-radius)#server 10.1.1.2 QTECH(config-gs-radius)#exit

	QTECH(config)#aaa group server radius g2 QTECH(config-gs-radius)#server 10.1.1.3 QTECH(config-gs-radius)#server 10.1.1.4 QTECH(config-gs-radius)#exit
Проверка	Запустите команды **show aaa group** и **show run** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa group Type Reference Name ---------- ---------- ---------- Radius 1 radius tacacs+ 1 tacacs+ radius 1 g1 radius 1 g2
	QTECH#show run ! radius-server host 10.1.1.1 radius-server host 10.1.1.2 radius-server host 10.1.1.3 radius-server host 10.1.1.4 radius-server key secret ! aaa group server radius g1 server 10.1.1.1 server 10.1.1.2 ! aaa group server radius g2 server 10.1.1.3 server 10.1.1.4 ! !

1.3.11.7. Распространенные ошибки

- Для серверов RADIUS, использующих порты аутентификации и учета не по умолчанию, при запуске команды **server** для добавления серверов укажите порт аутентификации или учета.
- Только группа серверов RADIUS может быть настроена с атрибутом VRF.

1.3.12. Настройка службы AAA на основе домена

1.3.12.1. Эффект конфигурации

Создавайте схемы AAA для пользователей 802.1X в разных доменах.

1.3.12.2. Примечания

О списках методов ссылок в доменах:

- Списки методов AAA, которые вы выбираете в режиме конфигурации домена, должны быть определены заранее. Если списки методов не определены заранее, при их выборе в режиме конфигурации домена система выдает сообщение о том, что конфигурации не существуют.
- Имена списков методов AAA, выбранных в режиме конфигурации домена, должны соответствовать именам списков методов, определенных для службы AAA. Если они несовместимы, служба AAA не может быть правильно предоставлена для пользователейв домене.

О домене по умолчанию:

- Домен по умолчанию: после включения службы AAA на основе домена, если имя пользователя не содержит информации о домене, служба AAA предоставляется пользователю на основе домена по умолчанию. Если информация о домене, переносимая именем пользователя, не настроена в системе, система определяет, что пользователь неавторизован и не будет предоставлять пользователю услугу AAA. Если домен по умолчанию изначально не настроен, его необходимо создать вручную.
- Когда служба AAA на основе домена включена, домен по умолчанию не настроен по умолчанию, и его необходимо создать вручную. Имя домена по умолчанию — **default**. Он используется для предоставления услуги AAA пользователям, имена пользователей которых не содержат информацию о домене. Если домен по умолчанию не настроен, служба AAA недоступна для пользователей, чьи имена пользователей не содержат информацию о домене.

О доменных именах:

- Имена доменов, содержащиеся в именах пользователей, и имена, настроенные на NAS, сопоставляются по принципу наибольшего совпадения.
- Если имя пользователя, прошедшего аутентификацию, содержит информацию о домене, но домен не настроен на NAS, услуга AAA пользователю не предоставляется.

1.3.12.3. Шаги настройки

Включение AAA

- Обязательный.
- Запустите команду **aaa new-model**, чтобы включить AAA.
- По умолчанию AAA отключен.

Включение службы AAA на основе домена

- Обязательный.
- Запустите команду **aaa domain enable**, чтобы включить службу AAA на основе домена.
- По умолчанию служба AAA на основе домена отключена.

Создание домена и вход в режим настройки домена

- Обязательный.
- Запустите команду **aaa domain**, чтобы создать домен, или войти в настроенный домен.
- По умолчанию домен не настроен.

Связывание домена со списком методов сетевого учета

- Запустите команду **accounting network**, чтобы связать домен с методом сетевого учета.
- Эта конфигурация является обязательной, если вам нужно применить к домену указанный список методов сетевого учета.
- Если домен не связан со списком методов сетевого учета, по умолчанию для учета используется глобальный список методов по умолчанию.

Связывание домена со списком методов сетевой авторизации

- Запустите команду **authorization network**, чтобы связать домен со списком методов сетевой авторизации.
- Эта конфигурация является обязательной, если вам нужно применить к домену указанный список методов сетевой авторизации.
- Если домен не связан со списком методов сетевой авторизации, по умолчанию для авторизации используется глобальный список методов по умолчанию.

Настройка статуса домена

- Опционально.
- Когда домен находится в состоянии блокировки, пользователи домена не могут войти в систему.
- По умолчанию после создания домена он находится в состоянии Активен, что указывает на то, что всем пользователям в домене разрешено запрашивать сетевые службы.

Настройка того, следует ли содержать доменное имя в именах пользователей

- Опционально.
- По умолчанию имена пользователей, которыми обмениваются NAS и сервер аутентификации, содержат информацию о домене.

Настройка максимального количества пользователей домена

- Опционально.
- По умолчанию максимальное количество пользователей доступа, разрешенных в домене, не ограничено.

1.3.12.4. Проверка

Запустите команду **show aaa domain**, чтобы проверить конфигурацию.

1.3.12.5. Связанные команды

Включение AAA

Команда	**aaa new-model**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы включить службы AAA, выполните эту команду. Ни одна из остальных команд AAA не может быть эффективной, если AAA не включена

Включение службы AAA на основе домена

Команда	**aaa domain enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы включить службу AAA на основе домена

Создание домена и вход в режим настройки домена

Команда	**aaa domain** { **default** | *domain-name* }
Описание параметров	**default**: этот параметр используется для настройки домена по умолчанию. *domain-name*: указывает имя создаваемого домена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы настроить домен для предоставления службы AAA на основе домена. Параметр **default** указывает домен по умолчанию. Если имя пользователя не содержит информации о домене, NAS использует список методов, связанный с доменом по умолчанию, для предоставления пользователю услуги AAA. Параметр *domain-name* указывает имя создаваемого домена. Если доменное имя, переносимое именем пользователя, совпадает с настроенным доменным именем, NAS использует список методов, связанный с этим доменом, для предоставления пользователю услуги AAA. Система поддерживает максимум 32 домена

Связывание домена со списком методов сетевого учета

Команда	accounting network { **default** | *list-name* }
Описание параметров	**default**: указывает, что используется список методов по умолчанию. *list-name*: указывает имя списка методов, который необходимо связать
Командный режим	Режим конфигурации домена
Руководство по использованию	Используйте эту команду, чтобы связать домен со списком методов сетевого учета

Связывание домена со списком методов авторизации в сети

Команда	**authorization network** { **default** | *list-name* }
Описание параметров	**default**: указывает, что используется список методов по умолчанию. *list-name*: указывает имя списка методов, который необходимо связать
Командный режим	Режим конфигурации домена

Настройка статуса домена

Команда	**state** { **block** | **active** }
Описание параметров	**block**: указывает, что настроенный домен недействителен. **active**: указывает, что настроенный домен действителен
Командный режим	Режим конфигурации домена
Руководство по использованию	Используйте эту команду, чтобы сделать настроенный домен действительным или недействительным

Настройка того, следует ли содержать доменное имя в именах пользователей

Команда	**username-format** { **without-domain** | **with-domain** }
Описание параметров	**without-domain**: указывает на удаление информации о домене из имен пользователей. **with-domain**: указывает, что в именах пользователей должна храниться информация о домене

Командный режим	Режим конфигурации домена
Руководство по использованию	Используйте эту команду в режиме конфигурации домена, чтобы определить, следует ли включать информацию о домене в имена пользователей, когда NAS взаимодействует с серверами аутентификации в указанном домене

Настройка максимального количества пользователей домена

Команда	**access-limit** *num*
Описание параметров	*num*: указывает максимальное количество пользователей доступа, разрешенных в домене. Это ограничение применимо только к STA 802.1X
Командный режим	Режим конфигурации домена
Руководство по использованию	Используйте эту команду, чтобы ограничить количество пользователей доступа в домене

1.3.12.6. Пример конфигурации

Настройка служб AAA на основе домена

Настройте аутентификацию и учет через сервер RADIUS для пользователей 802.1X (имя пользователя: user@domain.com), которые получают доступ к NAS. Имена пользователей, которые NAS отправляет на сервер RADIUS, не содержат информации о домене, и количество пользователей доступа не ограничено.

Сценарий:



Рисунок 1-13.

Шаги настройки	В следующем примере показано, как настроить аутентификацию и учет RADIUS, для чего требуется предварительная настройка сервера RADIUS. **Шаг 1.** Включите AAA. **Шаг 2.** Определите список методов AAA. **Шаг 3.** Включите службу AAA на основе домена. **Шаг 4.** Создайте домен. **Шаг 5.** Свяжите домен со списком методов AAA. **Шаг 6.** Настройте атрибут домена

NAS	QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key test QTECH(config)#aaa authentication dot1x default group radius QTECH(config)#aaa accounting network list3 start-stop group radius QTECH(config)# aaa domain enable QTECH(config)# aaa domain domain.com QTECH(config-aaa-domain)# authentication dot1x default QTECH(config-aaa-domain)# accounting network list3 QTECH(config-aaa-domain)# username-format without-domain
Проверка	Запустите команду **show run** и **show aaa domain** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#show aaa domain domain.com ==========Domain domain.com========== State: Active Username format: With-domain Access limit: No limit 802.1X Access statistic: 0 Selected method list: authentication dot1x default accounting network list3
	QTECH#show run Building configuration... co-operate enable ! aaa new-model aaa domain enable ! aaa domain domain.com authentication dot1x default accounting network list3

```
!
aaa accounting network list3 start-stop group radius
aaa authentication dot1x default group radius
!
nfpp
!
no service password-encryption
!
radius-server host 10.1.1.1
radius-server key test
!
line con 0
line vty 0 4
!
end
```

1.3.13. Настройка переключателя входа в систему для slave-устройства AAA

1.3.13.1. Эффект конфигурации

Когда переключатель включен, slave-устройству разрешается войти в систему; в противном случае slave-устройство не сможет войти в систему.

Конфигурация остается в силе, пока не будут внесены изменения.

1.3.13.2. Примечания

Сначала следует запустить команду **aaa new-model**.

1.3.13.3. Шаги настройки

Настройка переключателя входа в систему для slave-устройства AAA

- Необязательный.
- По умолчанию slave-устройству не разрешен вход в систему.

1.3.13.4. Проверка

Запустите команду **show run**, чтобы проверить конфигурацию.

1.3.13.5. Связанные команды

Настройка переключателя входа в систему для slave-устройства AAA

Команда	**aaa slave-login allow**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	По умолчанию переключатель выключен, поэтому slave-устройству не разрешен вход в систему. Когда переключатель включен, slave-устройство может войти в систему

1.3.13.6. Пример конфигурации

Настройка переключателя входа в систему для slave-устройства AAA

Сценарий:



Рисунок 1-14.

Шаги настройки	В следующем примере показано, как настроить переключатель входа в систему для slave-устройства AAA. **Шаг 1.** Включите AAA. **Шаг 2.** Включите переключатель входа в систему
NAS	QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#aaa slave-login allow
Проверка	Запустите команду **show run** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#sh run | inc aaa
	aaa new-model aaa slave-login allow

1.3.14. Настройка кеширования результатов авторизации

1.3.14.1. Эффект конфигурации

После настройки этой функции модуль AAA кеширует результаты авторизации, возвращенные с сервера. Поэтому более поздние авторизации на том же уровне могут выполняться на основе кеша.

1.3.14.2. Примечания

Кешированные результаты авторизации, происходящие из определенных уровней сеансов и команд, могут применяться только к сеансам и командам этих уровней.

1.3.14.3. Шаги настройки

Настройка кеширования результатов авторизации

- Опционально.
- По умолчанию результаты авторизации не кешируются.

1.3.14.4. Проверка

Запустите команду **show run**, чтобы проверить конфигурацию.

1.3.14.5. Связанные команды

Настройка кеширования результатов авторизации

Команда	**aaa command-author cache**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Устройство AAA кеширует результаты авторизации, возвращенные с сервера. Следовательно, более поздние авторизации на том же уровне могут выполняться на основе кешированных ресурсов

1.3.14.6. Пример конфигурации

Настройка кеширования результатов авторизации

Сценарий:



Рисунок 1-15.

Шаги настройки	В следующем примере показано, как настроить кеширование результатов авторизации **Шаг 1.** Включите AAA. **Шаг 2.** Включите переключатель входа в систему. **Шаг 3.** Настройте кеширование результатов авторизации
NAS	QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#aaa command-author cache QTECH(config)# aaa authorization commands 15 default group tacacs+

Проверка	Запустите команду **show run** на NAS, чтобы отобразить конфигурацию
NAS	QTECH#sh run | inc aaa
	aaa new-model aaa authorization commands 15 default group tacacs+ aaa command-author cache

1.4. Мониторинг

1.4.1. Очистка

Описание	Команда
Очищает заблокированных пользователей	**clear aaa local user lockout** {**all** | *user-name username* }

1.4.2. Отображение

Описание	Команда
Отображает информацию об обновлении учета	**show aaa accounting update**
Отображает текущую конфигурацию домена	**show aaa domain**
Отображает текущую конфигурацию блокировки	**show aaa lockout**
Отображает группы серверов AAA	**show aaa group**
Отображает списки методов AAA	**show aaa method-list**
Отображает пользователей AAA	**show aaa user**

2. НАСТРОЙКА RADIUS

2.1. Обзор

Служба удаленной аутентификации пользователей с телефонным подключением (RADIUS) представляет собой распределенную систему клиент/сервер.

RADIUS работает с аутентификацией, авторизацией и учетом (AAA) для проведения аутентификации пользователей, пытающихся получить доступ к сети, для предотвращения несанкционированного доступа. В реализации ПО клиент RADIUS запускается на устройстве или сервере доступа к сети (NAS) и передает запросы аутентификации на центральный сервер RADIOUS, где хранится вся информация об аутентификации пользователя и информация о сетевых службах. Помимо службы аутентификации сервер RADIUS предоставляет службы авторизации и учета для пользователей доступа.

RADIUS часто применяется в сетевых средах с высокими требованиями к безопасности и допускает доступ удаленных пользователей. RADIUS является полностью открытым протоколом, и сервер RADIUS устанавливается во многих операционных системах как компонент, например, в UNIX, Windows 2000 и Windows 2008. Таким образом, RADIUS является наиболее широко применяемым сервером безопасности в настоящее время.

Расширения динамической авторизации для службы удаленной аутентификации пользователей с набором номера определены в IETF RFC3576. Этот протокол определяет метод автономного управления пользователем. Устройства взаимодействуют с сервером RADIUS через сообщения об отключении (DM), чтобы отключить аутентифицированных пользователей. Этот протокол реализует совместимость между устройствами разных производителей и сервером RADIUS с точки зрения автономной обработки пользователей.

В механизме DM сервер RADIUS активно инициирует автономный запрос пользователя к устройству, устройство находит пользователя в соответствии с информацией о сеансе пользователя, именем пользователя и другой информацией, содержащейся в запросе, и переводит пользователя в автономный режим. Затем устройство возвращает ответный пакет, который переносит результат обработки на сервер RADIUS, тем самым реализуя автономное управление пользователями сервера RADIUS.

2.1.1. Протоколы и стандарты

- RFC2865: служба удаленной аутентификации пользователей по телефону (RADIUS).
- RFC2866: учет RADIUS.
- RFC2867: модификации учета RADIUS для поддержки туннельного протокола.
- RFC2869: расширения RADIUS.
- RFC3576: расширения динамической авторизации для службы удаленной аутентификации пользователей по телефону (RADIUS).

2.2. Приложения

Приложение	Описание
Предоставление услуг аутентификации, авторизации и учета для пользователей доступа	Аутентификация, авторизация и учет проводятся для пользователей, осуществляющих доступ в сети, для предотвращения несанкционированного доступа или операций
Принуждение пользователей к отключению от сети	Сервер заставляет аутентифицированного пользователя отключиться

2.2.1. Предоставление услуг аутентификации, авторизации и учета для пользователей доступа

2.2.1.1. Сценарий

RADIUS обычно применяется для аутентификации, авторизации и учета пользователей доступа. Сетевое устройство выступает в качестве клиента RADIUS и передает информацию о пользователе на сервер RADIUS. После завершения обработки сервер RADIUS возвращает клиенту RADIUS информацию о принятии/отказе аутентификации/ответе учета. Клиент RADIUS выполняет обработку пользователя доступа в соответствии с ответом сервера RADIUS.

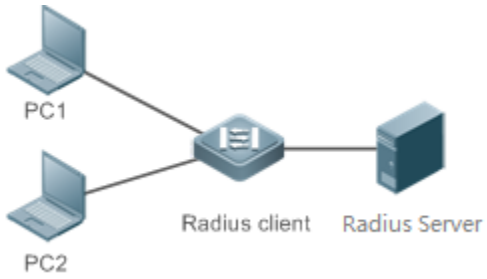


Рисунок 2-1. Типичная топология сети RADIUS

ПК 1 и ПК 2 подключаются к клиенту RADIUS в качестве пользователей доступа в проводном или беспроводном режиме и инициируют запросы аутентификации и учета.

Клиент RADIUS обычно является коммутатором доступа или коммутатором агрегации.

Сервер RADIUS может быть компонентом, встроенным в операционную систему Windows Server (IAS) или UNIX, или программным обеспечением выделенного сервера, предоставляемым поставщиками.

2.2.1.2. Развертывание

- Настройте информацию об устройстве доступа на сервере RADIUS, включая IP-адрес и совместный ключ устройств доступа.
- Настройте список методов AAA на клиенте RADIUS.
- Настройте информацию о сервере RADIUS на клиенте RADIUS, включая IP-адрес и совместный ключ.
- Включите контроль доступа на порту доступа клиента RADIUS.

- Настройте сеть так, чтобы клиент RADIUS успешно взаимодействовал с сервером RADIUS.

2.2.2. Принуждение пользователей к отключению от сети

2.2.2.1. Сценарий

Сервер RADIUS вынуждает аутентифицированных онлайн-пользователей отключаться от сети ради управления.

Смотрите Рисунок 2-1 для понимания топологии сети.

2.2.2.2. Развертывание

- Добавьте следующее развертывание на основе раздела Настройка AAA в однодоменной среде.
- Включите функцию расширения динамической авторизации RADIUS на клиенте RADIUS.

2.3. Функции

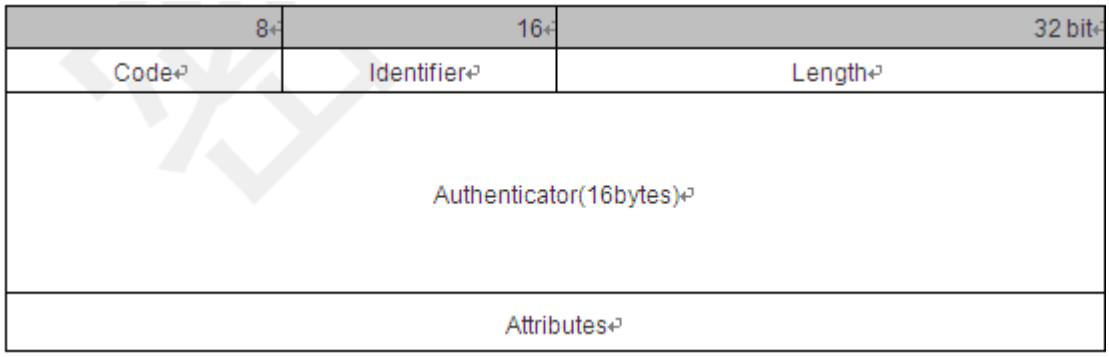
2.3.1. Базовые концепты

Режим клиент/сервер

- Клиент: клиент RADIUS инициирует запросы RADIUS и обычно работает на устройстве или NAS. Он передает информацию о пользователе на сервер RADIUS, получает ответы от сервера RADIUS и выполняет соответствующую обработку. Обработка включает в себя принятие доступа пользователя, отклонение доступа пользователя или сбор дополнительной информации о пользователе для сервера RADIUS.
- Сервер: несколько клиентов RADIUS сопоставляются с одним сервером RADIUS. Сервер RADIUS поддерживает IP-адреса и совместные ключи всех клиентов RADIUS, а также информацию обо всех аутентифицированных пользователях. Он получает запросы от клиента RADIUS, выполняет аутентификацию, авторизацию и учет и возвращает информацию об обработке клиенту RADIUS.

Структура пакетов RADIUS

На следующем рисунке показана структура пакетов RADIUS.



- Код (Code): определяет тип пакетов RADIUS, который занимает один байт. В следующей таблице перечислены значения и определения.

Код	Тип пакета	Код	Тип пакета
1	Доступ-Запрос	4	Учет-Запрос
2	Доступ-Принять	5	Учет-Ответ
3	Доступ-Отклонить	11	Доступ-Вызов

- Идентификатор (Identifier): указывает идентификатор для сопоставления пакетов запроса и пакетов ответа, который занимает один байт. Значения идентификаторов пакетов запросов и пакетов ответов одного типа одинаковы.
- Длина (Length): определяет длину всего пакета RADIUS, включая код, идентификатор, длину, аутентификатор и атрибуты. Он занимает два байта. Байты, выходящие за пределы поля «Длина», будут усечены. Если длина полученного пакета меньше значения параметра «Длина», пакет отбрасывается.
- Аутентификатор (Authenticator): проверяет пакеты ответа сервера RADIUS клиентом RADIUS, который занимает 16 байт. Это поле также используется для шифрования/дешифрования паролей пользователей.
- Атрибуты (Attributes): содержит аутентификационную, авторизационную и учетную информацию, длина не фиксирована. Поле «Атрибуты» обычно содержит несколько атрибутов. Каждый атрибут представлен в формате Type, Length, Value (TLV). Тип занимает один байт и указывает тип атрибута. В следующей таблице перечислены общие атрибуты аутентификации, авторизации и учета RADIUS. Длина занимает один байт и указывает длину атрибута в байтах. Значение указывает информацию атрибута.

Атрибут №	Имя атрибута	Атрибут №	Имя атрибута
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count

Атрибут №	Имя атрибута	Атрибут №	Имя атрибута
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry

Атрибут №	Имя атрибута	Атрибут №	Имя атрибута
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

Совместный ключ

Клиент RADIUS и сервер RADIUS взаимно подтверждают свои дентификационные данные, используя совместный ключ во время связи. Совместный ключ не может быть передан по сети. Кроме того, пароли пользователей шифруются для передачи в целях безопасности.

Группа серверов RADIUS

Протокол безопасности RADIUS, также называемый методом RADIUS, настраивается в виде группы серверов RADIUS. Каждый метод RADIUS соответствует одной группе серверов RADIUS, и в одну группу серверов RADIUS можно добавить один или несколько серверов RADIUS. Подробнее о методе RADIUS см. в разделе Настройка AAA. Если вы добавляете несколько серверов RADIUS в одну группу серверов RADIUS, когда связь между устройством и первым сервером RADIUS в этой группе прерывается или первый сервер RADIUS становится недоступным, устройство автоматически пытается установить связь со следующим сервером RADIUS до тех пор, пока связь не будет установлена. успешно, или связь со всеми серверами RADIUS не удалась.

Тип атрибута RADIUS

- Стандартные атрибуты
- Стандарты RFC определяют номера и содержимое атрибутов RADIUS, но не определяют формат некоторых типов атрибутов. Следовательно, формат содержимого атрибута необходимо настроить для адаптации к различным требованиям сервера RADIUS. В настоящее время можно настроить формат атрибута RADIUS Calling-Station-ID (атрибут №: 31).

Атрибут RADIUS Calling-Station-ID используется для идентификации пользователей, когда сетевое устройство передает пакеты запросов на сервер RADIUS. Атрибут RADIUS Calling-Station-ID представляет собой строку, которая может принимать несколько форматов. Он должен однозначно идентифицировать пользователя. Поэтому часто задается MAC-адрес пользователя. Например, при использовании аутентификации IEEE 802.1X атрибут Calling-Station-ID устанавливается равным MAC-адресу устройства, на котором установлен клиент IEEE 802.1X. В следующей таблице описывается формат MAC-адресов.

Формат	Описание
Ietf	Указывает стандартный формат, указанный в стандарте IETF (RFC3580), который разделен разделителем (-). Пример: 08-c6-b3-33-22-AC
Нормальный (Normal)	Указывает общий формат, представляющий MAC-адрес (шестнадцатеричный формат с точками), разделенный разделителем (.). Пример: 08c6.b333.22ac
Неформатированный (Unformatted)	Указывает формат без разделителей. Этот формат используется по умолчанию. Пример: 08c6b33322ac

- Приватные атрибуты

RADIUS — это расширяемый протокол. Согласно RFC2865 атрибут Vendor-Specific (атрибут №: 26) используется поставщиками устройств для расширения протокола RADIUS для реализации приватных функций или функций, которые не определены в стандартном протоколе RADIUS. В Таблице ниже перечислены приватные атрибуты, поддерживаемые продуктами QTECH. В столбце «Тип» указана конфигурация приватных атрибутов продуктов QTECH по умолчанию, а в столбце «Расширенный тип» указана конфигурация приватных атрибутов других продуктов, не принадлежащих QTECH, по умолчанию.

ID	Функция	Тип	Расширенный тип
1	max-down-rate	1	76
2	port-priority	2	77

ID	Функция	Тип	Расширенный тип
3	user-ip	3	3
4	vlan-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42

ID	Функция	Тип	Расширенный тип
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

2.3.2. Обзор

Особенность	Описание
RADIUS-аутентификация, авторизация и учет	Проводит аутентификацию личности и учет пользователей доступа, обеспечивает сетевую безопасность и упрощает управление для сетевых администраторов
Исходный адрес пакетов RADIUS	Указывает исходный IP-адрес, используемый клиентом RADIUS для передачи пакетов на сервер RADIUS
Тайм-аут повторной передачи RADIUS	Указывает параметр повторной передачи пакетов для клиента RADIUS, когда сервер RADIUS не отвечает на пакеты, переданные от клиента RADIUS, в течение определенного периода времени
Обнаружение доступности сервера RADIUS	Позволяет клиенту RADIUS активно определять, доступен ли сервер RADIUS, и поддерживать доступность каждого сервера RADIUS. Доступный RADIUS-сервер выбирается предпочтительно для повышения производительности обработки служб RADIUS
Принудительный автономный режим RADIUS	Включает RADIUS-сервер для принудительного отключения аутентифицированных пользователей

2.3.3. RADIUS-аутентификация, авторизация и учет

Выполняйте аутентификацию и учет пользователей доступа, защищайте сетевую безопасность и облегчайте управление для сетевых администраторов.

2.3.3.1. Принцип работы

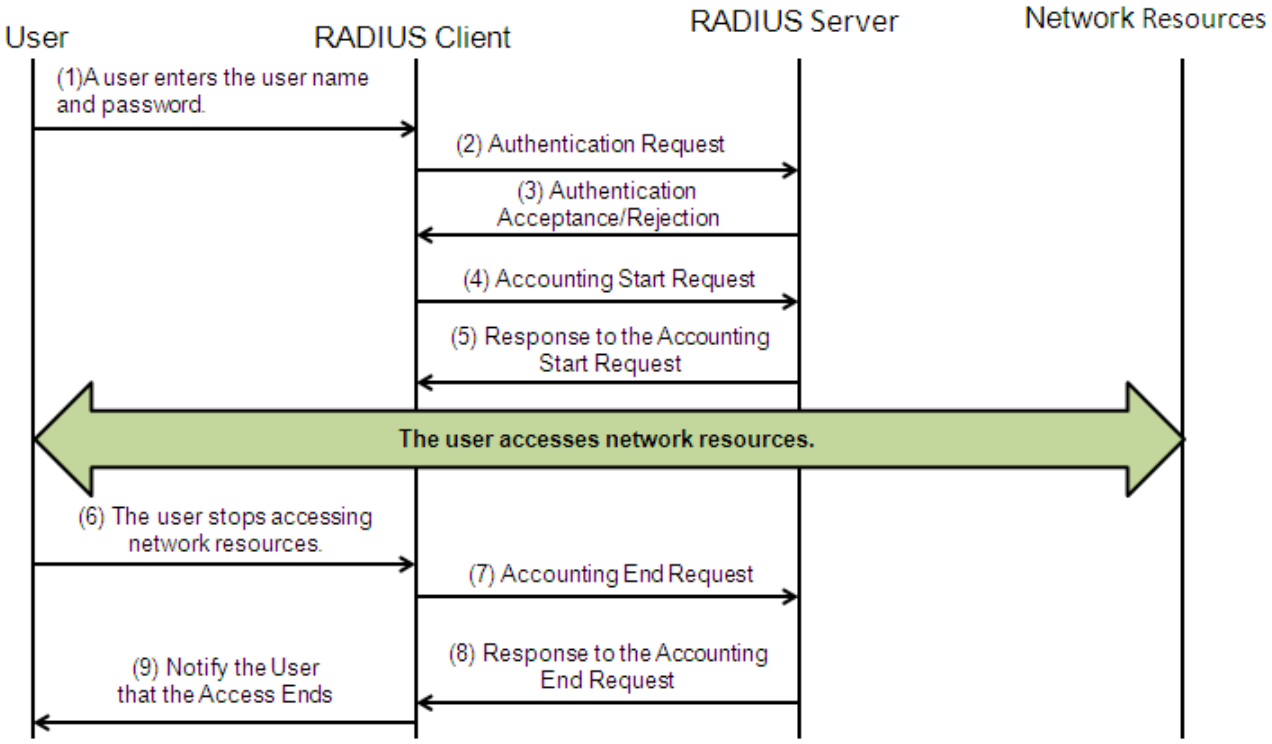


Рисунок 2-2.

Процесс аутентификации и авторизации RADIUS описывается следующим образом:

1. Пользователь вводит имя пользователя и пароль и передает их клиенту RADIUS.
2. После получения имени пользователя и пароля клиент RADIUS передает пакет запроса аутентификации на сервер RADIUS. Пароль шифруется для передачи. Для метода шифрования см. RFC2865.
3. Сервер RADIUS принимает или отклоняет запрос аутентификации в соответствии с именем пользователя и паролем. При приеме запроса на аутентификацию сервер RADIUS также выдает информацию об авторизации помимо информации о принятии аутентификации. Информация об авторизации зависит от типа пользователей доступа.

Процесс учета RADIUS описывается следующим образом:

1. Если сервер RADIUS возвращает информацию о принятии аутентификации на шаге (3), клиент RADIUS немедленно отправляет пакет запроса на запуск учета на сервер RADIUS.
2. Сервер RADIUS возвращает ответный пакет о начале учета, указывающий на начало учета.
3. Пользователь прекращает доступ к сетевым ресурсам и запрашивает у RADIUS-клиента отключение сетевого подключения.
4. Клиент RADIUS передает пакет запроса завершения учета на сервер RADIUS.
5. Сервер RADIUS возвращает ответный пакет учета, указывающий на завершение учета.
6. Пользователь отключен и не может получить доступ к сетевым ресурсам.

2.3.3.2. Связанная конфигурация

Настройка параметров RADIUS-сервера

По умолчанию сервер RADIUS не настроен.

Вы можете запустить команду **radius-server host** для настройки сервера RADIUS.

По крайней мере один сервер RADIUS должен быть настроен для нормальной работы служб RADIUS.

Настройка списка методов аутентификации AAA

По умолчанию список методов аутентификации AAA не настроен.

Вы можете запустить команду **aaa authentication**, чтобы настроить список методов для разных типов пользователей и выбрать **group radius** при настройке метода аутентификации.

Аутентификация RADIUS может быть выполнена только после настройки списка методов аутентификации AAA для соответствующих типов пользователей.

Настройка списка методов авторизации AAA

По умолчанию список методов авторизации AAA не настроен.

Вы можете запустить команду **aaa authorization**, чтобы настроить список методов авторизации для разных типов пользователей и выбрать **group radius** при настройке метода авторизации.

Авторизация RADIUS может быть выполнена только после настройки списка методов авторизации AAA для соответствующих типов пользователей.

Настройка списка методов учета AAA

По умолчанию список методов учета AAA не настроен.

Вы можете запустить команду **aaa accounting**, чтобы настроить список методов учета для разных типов пользователей и выбрать **group radius** при настройке метода учета.

Учет RADIUS можно вести только после настройки списка методов учета AAA для соответствующих типов пользователей.

2.3.4. Исходный адрес пакетов RADIUS

Укажите исходный IP-адрес, используемый клиентом RADIUS для передачи пакетов на сервер RADIUS.

2.3.4.1. Принцип работы

При настройке RADIUS укажите исходный IP-адрес, который будет использоваться RADIUS-клиентом для передачи RADIUS-пакетов на RADIUS-сервер, чтобы снизить рабочую нагрузку, связанную с хранением большого объема информации NAS на RADIUS-сервере.

2.3.4.2. Связанная конфигурация

Глобальная маршрутизация используется для определения исходного адреса для передачи пакетов RADIUS по умолчанию.

Запустите команду **ip radius source-interface**, чтобы указать исходный интерфейс для передачи пакетов RADIUS. Устройство использует первый IP-адрес указанного интерфейса в качестве исходного адреса пакетов RADIUS.

2.3.5. Тайм-аут повторной передачи RADIUS

2.3.5.1. Принцип работы

После того, как клиент RADIUS передает пакет на сервер RADIUS, запускается таймер для обнаружения ответа сервера RADIUS. Если сервер RADIUS не отвечает в течение определенного периода времени, клиент RADIUS повторно передает пакет.

2.3.5.2. Связанная конфигурация

Настройка тайм-аута сервера RADIUS

Тайм-аут по умолчанию составляет 5 секунд.

Вы можете запустить команду **radius-server timeout**, чтобы настроить время тайм-аута. Значение варьируется от 1 секунды до 1000 секунд.

Время отклика сервера RADIUS зависит от его производительности и сетевой среды. Установите подходящий тайм-аут в соответствии с фактическими условиями.

Настройка счетчика повторных передач

Количество повторных передач по умолчанию равно 3.

Вы можете запустить команду **radius-server retransmit**, чтобы настроить количество повторных передач. Значение варьируется от 1 до 100.

Настройка необходимости повторной передачи пакетов обновления учета

Пакеты обновления учета не передаются повторно по умолчанию.

Вы можете запустить команду **radius-server account update retransmit**, чтобы настроить повторную передачу пакетов обновления учетной записи для пользователей, прошедших аутентификацию.

2.3.6. Обнаружение доступности сервера RADIUS

2.3.6.1. Принцип работы

Клиент RADIUS активно определяет, доступен ли сервер RADIUS, и поддерживает доступность каждого сервера RADIUS. Доступный RADIUS-сервер выбирается предпочтительно для повышения производительности обработки служб RADIUS.

2.3.6.2. Связанная конфигурация

Настройка критериев, по которым устройство определяет, что сервер RADIUS недоступен

Критерии по умолчанию, настроенные для оценки того, что сервер RADIUS недоступен, одновременно удовлетворяют двум условиям: 1. Устройство не получает корректный ответный пакет от сервера безопасности RADIUS в течение 60 секунд. 2. Устройство передает пакет запроса на один и тот же сервер безопасности RADIUS 10 раз подряд.

Вы можете запустить команду **radius-server dead-criteria**, чтобы настроить критерии, по которым устройство будет определять, что сервер безопасности RADIUS недоступен.

Настройка имени тестового пользователя для активного обнаружения сервера безопасности RADIUS

По умолчанию имя тестового пользователя для активного обнаружения сервера безопасности RADIUS не указано.

Вы можете запустить команду **radius-server host x.x.x.x testusername xxx**, чтобы настроить тестовое имя пользователя.

2.3.7. Принудительный автономный режим RADIUS

2.3.7.1. Принцип работы

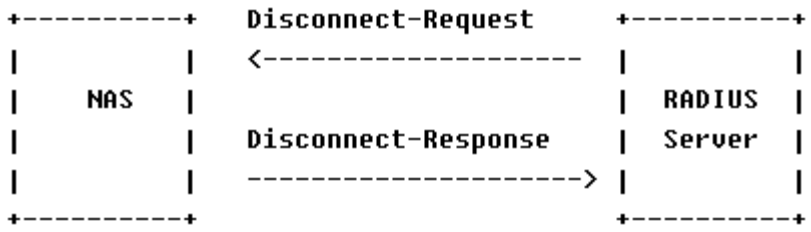


Рисунок 2-3. Обмен сообщениями DM протокола расширения динамической авторизации RADIUS

На предыдущем Рисунке показан обмен сообщениями DM между сервером RADIUS и устройством. Сервер RADIUS передает сообщение Disconnect-Request на UDP-порт 3799 устройства. После обработки устройство возвращает сообщение Disconnect-Response, которое переносит результат обработки на сервер RADIUS.

2.3.7.2. Связанная конфигурация

Н/Д

2.4. Конфигурация

Конфигурация	Описание и команда	
Базовая конфигурация RADIUS	(Обязательно) Используется для настройки аутентификации, авторизации и учета RADIUS	
	radius-serverhost	Настраивает IP-адрес удаленного сервера безопасности RADIUS
	radius-serverkey	Настраивает совместный ключ для связи между устройством и сервером RADIUS
	radius-serverretransmit	Настраивает количество передач запроса, после чего устройство подтверждает, что сервер RADIUS недоступен
	radius-servertimeout	Настраивает время ожидания, по истечении которого устройство повторно передает запрос

Конфигурация	Описание и команда	
Базовая конфигурация RADIUS	**radius-server account update retransmit**	Настраивает повторную передачу пакетов обновления учета для аутентифицированных пользователей
	ip radius source-interface	Настраивает исходный адрес пакетов RADIUS
Настройка типа атрибута RADIUS	(Опционально) Он используется для определения обработки атрибутов, принятой, когда устройство инкапсулирует и анализирует пакеты RADIUS	
	radius-serverattribute31	Настраивает формат MAC-адреса атрибута RADIUS № 31 (Calling-Station-ID)
	radius set qoscos	Устанавливает приватный атрибут port-priority, выдаваемый сервером, равным значению COS интерфейса. Концепции, относящиеся к COS, см. в разделе ACL&QoS Configuration/ Настройка QoS
	radius support cui	Настраивает устройство для поддержки атрибута CUI
	radius vendor-specific	Настраивает режим разбора приватных атрибутов устройством
Настройка обнаружения доступности RADIUS	(Опционально) Используется для определения доступности сервера RADIUS и поддержания доступности RADIUS-сервера	
	radius-server dead-criteria	Настраивает глобальные критерии для определения того, что сервер безопасности RADIUS недоступен
	radius-server deadtime	Настраивает продолжительность, в течение которой устройство прекращает передачу пакетов запросов на недостижимый сервер RADIUS
	radius-server host	Настраивает IP-адрес удаленного сервера безопасности RADIUS, порт аутентификации, порт учета и параметры активного обнаружения

2.4.1. Базовая конфигурация RADIUS

2.4.1.1. Эффект конфигурации

Аутентификация, авторизация и учет RADIUS могут выполняться после завершения базовой настройки RADIUS.

2.4.1.2. Примечания

- Перед настройкой RADIUS на устройстве убедитесь, что сетевое соединение сервера RADIUS находится в хорошем состоянии.
- При выполнении команды **ip radius source-interface** для настройки исходного адреса пакетов RADIUS убедитесь, что устройство исходного IP-адреса успешно взаимодействует с сервером RADIUS.

2.4.1.3. Шаги настройки

Настройка удаленного сервера безопасности RADIUS

- Обязательный.
- Настройте IP-адрес, порт аутентификации, порт учета и совместный ключ сегмента сервера безопасности RADIUS.

Настройка совместный ключа для связи между устройством и сервером RADIUS

- Опционально.
- Настройте совместный ключ в режиме глобальной конфигурации для серверов без общего ключа.

ПРИМЕЧАНИЕ: совместный ключ на устройстве должен совпадать с ключом на сервере RADIUS.

Настройка счетчика передачи запроса, после которого устройство подтверждает, что сервер RADIUS недоступен

- Опционально.
- Настройте счетчик передачи запроса, после которого устройство подтверждает, что сервер RADIUS недоступен, в соответствии с реальной сетевой средой.

Настройка времени ожидания, по истечении которого устройство повторно передает запрос

- Опционально.
- Настройте время ожидания, по истечении которого устройство повторно передает запрос, в соответствии с реальной сетевой средой.

ПРИМЕЧАНИЕ: в среде аутентификации 802.1X, использующей протокол безопасности RADIUS, если сетевое устройство служит аутентификатором 802.1X, а QTECH SU используется в качестве клиентского программного обеспечения 802.1X, рекомендуется установить тайм-аут RADIUS-сервера на 3 секунды (значение по умолчанию — 5 секунд), а повторная передача RADIUS-сервера — 2 (значение по умолчанию — 3) на сетевом устройстве.

Настройка исходного адреса пакетов RADIUS

- Опционально.
- Настройте исходный адрес пакетов RADIUS в соответствии с реальной сетевой средой.

2.4.1.4. Проверка

- Настройте список методов AAA, указывающий на выполнение идентификации, авторизации и учета пользователей с помощью RADIUS.
- Включите взаимодействие устройства с сервером RADIUS. Выполните захват пакетов, чтобы убедиться, что устройство обменивается данными с сервером RADIUS по протоколу RADIUS.

2.4.1.5. Связанные команды

Настройка удаленного сервера безопасности RADIUS

Команда	**radius-server host** [**oob** [**via** *mgmt_name*]] { *ipv4-address* } [**auth-port** *port-number*] [**acct-port** *port-number*][**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]
Описание параметров	**oob**: указывает аутентификацию oob, то есть исходным интерфейсом для передачи пакетов на сервер RADIUS является порт управления. **via** *mgmt_name*: указывает конкретный порт управления, если oob поддерживает несколько портов управления. *ipv4-address*: указывает IPv4-адрес сервера безопасности RADIUS. **auth-port** *port-number*: указывает порт UDP для аутентификации личности RADIUS. Диапазон значений от 0 до 65535. Если установлено значение 0, хост не выполняет аутентификацию личности. **acct-port** *port-number*: указывает порт UDP для учета RADIUS. Диапазон значений от 0 до 65 535. Если он установлен в 0, хост не ведет учет. **test username** *name*: включает функцию активного обнаружения сервера безопасности RADIUS и указывает имя пользователя, используемое для активного обнаружения. **idle-time** *time*: указывает интервал, в течение которого устройство должно передавать тестовые пакеты на доступный сервер безопасности RADIUS. Значение по умолчанию — 60 минут. Значение варьируется от 1 минуты до 1440 минут (24 часа). **ignore-auth-port**: отключает функцию определения порта аутентификации сервера безопасности RADIUS. Он включен по умолчанию. **ignore-acct-port**: отключает функцию обнаружения порта учета сервера безопасности RADIUS. Он включен по умолчанию. **key** [**0** | **7**] *text-string*: настраивает совместный ключ сервера. Глобальный совместный ключ используется, если он не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Сервер безопасности RADIUS должен быть определен для реализации службы безопасности AAA с использованием RADIUS. Вы можете запустить команду **radius-server host**, чтобы определить один или несколько серверов безопасности RADIUS. Если сервер безопасности

	RADIUS не добавлен в группу серверов RADIUS, устройство использует глобальную таблицу маршрутизации при передаче пакетов RADIUS на сервер RADIUS. В противном случае устройство использует таблицу маршрутизации VRF группы серверов RADIUS

Настройка общего ключа для связи между устройством и сервером RADIUS

Команда	**radius-server key** [**0** | **7**] *text-string*
Описание параметров	*text-string*: указывает текст общего ключа. **0 | 7**: указывает тип шифрования ключа. Значение 0 указывает на отсутствие шифрования, а 7 указывает на простое шифрование. Значение по умолчанию — 0
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Совместный ключ является основой для правильной связи между устройством и сервером безопасности RADIUS. Один и тот же совместный ключ должен быть настроен на устройстве и сервере безопасности RADIUS, чтобы они могли успешно взаимодействовать друг с другом

Настройка счетчика передачи запроса, после которого устройство подтверждает, что сервер RADIUS недоступен

Команда	**radius-server retransmit** *retries*
Описание параметров	*retries*: указывает количество повторных передач RADIUS. Значение варьируется от 1 до 100
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Предпосылкой для использования AAA следующего метода аутентификации пользователя является то, что текущий сервер безопасности, используемый для аутентификации, не отвечает. Критерием для устройства, чтобы определить, что сервер безопасности не отвечает, является то, что сервер безопасности не отвечает в течение продолжительности повторной передачи пакета RADIUS указанного счетчика повторных передач. Существует интервал между двумя последовательными повторными передачами

Настройка времени ожидания, по истечении которого устройство повторно передает запрос

Команда	**radius-server timeout** *seconds*
Описание параметров	*seconds*: указывает время ожидания в секундах. Значение варьируется от 1 секунды до 1000 секунд
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для настройки тайм-аута повторной передачи пакета

Настройка повторной передачи пакетов обновления учета для пользователей, прошедших проверку подлинности

Команда	**radius-server account update retransmit**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте повторную передачу пакетов обновления учета для пользователей, прошедших аутентификацию. Пакеты обновления учета не передаются повторно по умолчанию. Конфигурация не влияет на пользователей других типов

2.4.1.6. Пример конфигурации

Использование аутентификации, авторизации и учета RADIUS для пользователей, вошедших в систему

Сценарий:

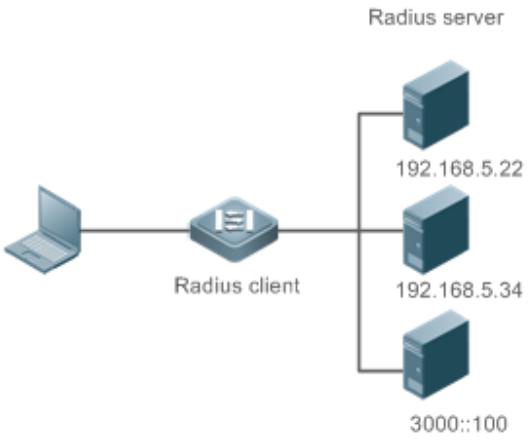


Рисунок 2-4.

Шаги настройки	• Включить AAA. • Настройте информацию о сервере RADIUS. • Настройте использование методов аутентификации, авторизации и учета RADIUS. • Примените настроенный метод аутентификации на интерфейсе
RADIUS-клиент	QTECH#configure terminal QTECH (config)#aaa new-model QTECH (config)# radius-server host 192.168.5.22 QTECH (config)#radius-server host 3000::100 QTECH (config)# radius-server key aaa QTECH (config)#aaa authentication login test group radius QTECH (config)#aaa authorizationexectest group radius QTECH (config)#aaa accountingexectest start-stop group radius QTECH (config)# line vty 0 4 QTECH (config-line)#login authentication test QTECH (config-line)# authorization exec test QTECH (config-line)# accounting exec test
Проверка	Telnet к устройству с ПК. Отображается экран с запросом имени пользователя и пароля. Введите правильное имя пользователя и пароль для входа в устройство. После получения определенного уровня доступа, предоставленного сервером, запускайте команды только под этим уровнем доступа. Отображение журнала аутентификации пользователя на сервере RADIUS. Выполняйте операции управления на устройстве от имени пользователя, а затем выйдите из системы. Отображает учетную информацию о пользователе на сервере RADIUS
	QTECH#show running-config ! radius-server host 192.168.5.22 radius-server host 3000::100 radius-server key aaa aaa new-model aaa accounting exec test start-stop group radius aaa authorization exec test group radius aaa authentication login test group radius no service password-encryption iptcp not-send-rst !

```
vlan 1
!
line con 0
line vty 0 4
accounting exec test
authorization exec test
login authentication test
!
```

2.4.1.7. Распространенные ошибки

- Ключ, настроенный на устройстве, не соответствует ключу, настроенному на сервере.
- Список методов не настроен.

2.4.2. Настройка типа атрибута RADIUS

2.4.2.1. Эффект конфигурации

Определите обработку атрибутов, принятую, когда устройство инкапсулирует и анализирует пакеты RADIUS.

2.4.2.2. Примечания

Приватные атрибуты, задействованные в разделе «Настройка типа атрибута RADIUS», относятся к приватным атрибутам QTECH.

2.4.2.3. Шаги настройки

Настройка формата MAC-адреса атрибута RADIUS № 31 (Calling-Station-ID)

- Опционально.
- Установите формат MAC-адреса Calling-Station-Id на тип, поддерживаемый сервером.

Настройка типа приватного атрибута RADIUS

- Опционально.
- Если сервер является сервером приложений QTECH, необходимо настроить приватный тип атрибута RADIUS.

Установка приоритета порта приватного атрибута, выдаваемого сервером, на значение COS интерфейса

- Опционально.
- При необходимости установите для приватного атрибута port-priority, выдаваемого сервером, значение COS интерфейса.

Настраивает устройство для поддержки атрибута CUI

- Опционально.
- При необходимости настройте, поддерживает ли устройство атрибут RADIUS CUI.

Настройка режима разбора приватных атрибутов устройством

- Опционально.

- Настройте индекс приватного атрибута QTECH, анализируемого устройством, как требуется.

2.4.2.4. Проверка

- Настройте список методов AAA, указывающий на выполнение идентификации, авторизации и учета пользователей с помощью RADIUS.
- Включите взаимодействие устройства с сервером RADIUS. Выполните захват пакетов, чтобы отобразить формат MAC-адреса Calling-Station-Id.
- Включите взаимодействие устройства с сервером RADIUS. Отобразите отладочную информацию устройства, чтобы убедиться, что приватные атрибуты QTECH правильно анализируются устройством.
- Включите взаимодействие устройства с сервером RADIUS. Отобразите отладочную информацию устройства, чтобы убедиться, что атрибут CUI правильно анализируется устройством.

2.4.2.5. Связанные команды

Настройка формата MAC-адреса атрибута RADIUS № 31 (Calling-Station-ID)

Команда	**radius-server attribute 31 mac format** {**ietf** | **normal** | **unformatted** }
Описание параметров	**ietf**: указывает стандартный формат, указанный в стандарте IETF (RFC3580), который разделен разделителем (-). Пример: 08-c6-b3-33-22-AC. **normal**: указывает общий формат, представляющий MAC-адрес (шестнадцатеричный формат с точками), разделенный разделителем (.). Пример: 08c6.b333.22ac. **unformatted**: указывает формат без разделителей. Этот формат используется по умолчанию. Пример: 08c6b33322ac
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Некоторые серверы безопасности RADIUS могут идентифицировать только MAC-адреса в формате IETF. В этом случае установите для формата MAC-адреса Calling-Station-ID значение IETF

Установка приоритета порта приватного атрибута, выдаваемого сервером, на значение COS интерфейса

Команда	**radius set qoscos**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте эту команду для использования выданного значения QoS в качестве значения CoS. Значение QoS используется в качестве значения DSCP по умолчанию

Настраивает устройство для поддержки атрибута CUI

Команда	**radius support cui**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте эту команду, чтобы разрешить RADIUS-совместимому устройству поддерживать атрибут CUI

Настройка режима разбора приватных атрибутов устройством

Команда	**radius vendor-specific extend**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы идентифицировать атрибуты всех идентификаторов поставщиков по типу

2.4.2.6. Пример конфигурации

Настройка типа атрибута RADIUS

Сценарий	Одна аутентификация устройство
Шаги настройки	• Настройте формат MAC-адреса RADIUS Calling-Station-Id. • Установите значение QoS, выданное сервером RADIUS, в качестве значения COS интерфейса. • Настройте функцию RADIUS для поддержки атрибута CUI. • Настройте устройство для поддержки приватных атрибутов других поставщиков
	QTECH(config)#radius-server attribute 31 mac format ietf QTECH(config)#radiussetqoscos QTECH(config)#radiussupport cui QTECH(config)#radiusvendor-specific extend
Проверка	Выполните захват пакетов или отобразите отладочную информацию устройства, чтобы проверить, правильно ли инкапсулированы/ анализированы стандартные атрибуты RADIUS и приватные атрибуты

2.4.3. Настройка обнаружения доступности RADIUS

2.4.3.1. Эффект конфигурации

Устройство поддерживает статус доступности каждого настроенного сервера RADIUS: доступен или недоступен. Устройство не будет передавать запросы аутентификации,

авторизации и учета пользователей на недоступный сервер RADIUS, если только все остальные серверы в той же группе серверов RADIUS, что и недоступный сервер, не будут недоступны.

Устройство активно обнаруживает указанный сервер RADIUS. Функция активного обнаружения отключена по умолчанию. Если активная функция обнаружения включена для указанного сервера RADIUS, устройство, в соответствии с конфигурацией, будет периодически передавать запросы обнаружения (запросы аутентификации или запросы учета) на сервер RADIUS. Интервал передачи следующий:

- Для доступного сервера RADIUS интервал — это активный интервал обнаружения доступного сервера RADIUS (значение по умолчанию — 60 минут).
- Для недоступного сервера RADIUS интервал всегда равен 1 минуте.

2.4.3.2. Примечания

Все следующие условия должны быть выполнены, прежде чем активная функция обнаружения будет включена для указанного сервера RADIUS:

- На устройстве настроено тестовое имя пользователя сервера RADIUS.
- На устройстве настроен как минимум один тестируемый порт (порт аутентификации или порт учета) RADIUS-сервера.

Если выполняются все следующие два условия, считается, что доступный сервер RADIUS становится недоступным:

- После того, как от сервера RADIUS был получен предыдущий правильный ответ, истекло время, установленное в **radius-server dead-criteria time** *seconds*.
- После того, как от сервера RADIUS получен предыдущий правильный ответ, количество попыток, когда устройство отправляет запросы на сервер RADIUS, но не получает правильных ответов (включая повторную передачу), достигает значения, установленного в **radius-server dead-criteria tries** *number*.

Если выполняется любое из следующих условий, считается, что недоступный сервер RADIUS становится доступным:

- Устройство получает правильные ответы от сервера RADIUS.
- Продолжительность, в течение которой RADIUS-сервер находится в состоянии недоступности, превышает время, установленное в **radius-server deadtime**, а функция активного обнаружения отключена для RADIUS-сервера.
- Порт аутентификации или порт учета сервера RADIUS обновляется на устройстве.

2.4.3.3. Шаги настройки

Настройка глобальных критериев для оценки того, что сервер безопасности RADIUS недоступен

- Обязательный.
- Настройка глобальных критериев для оценки того, что сервер безопасности RADIUS недоступен, является необходимым условием для включения функции активного обнаружения.

Настройка IP-адреса удаленного сервера безопасности RADIUS, порта аутентификации, порта учета и параметров активного обнаружения

- Обязательный.
- Настройка параметров активного обнаружения сервера RADIUS является необходимым условием для включения функции активного обнаружения.

Настройка продолжительности прекращения передачи устройством пакетов запросов на недоступный RADIUS-сервер

- Опционально.
- Настроенная продолжительность, в течение которой устройство прекращает передачу пакетов запросов на недоступный сервер RADIUS, вступает в силу только в том случае, если функция активного обнаружения отключена для сервера RADIUS.

2.4.3.4. Проверка

Запустите команду **show radius server**, чтобы отобразить информацию о доступности каждого сервера RADIUS.

2.4.3.5. Связанные команды

Настройка глобальных критериев для оценки того, что сервер безопасности RADIUS недоступен

Команда	**radius-server dead-criteria** { **time** *seconds* [**tries** *number*] | **tries** *number* }
Описание параметров	**time** *seconds*: указывает параметр условия времени. Если устройство не может получить правильный ответный пакет от сервера безопасности RADIUS в течение указанного времени, считается, что сервер безопасности RADIUS удовлетворяет условию продолжительности недоступности. Значение варьируется от 1 секунды до 120 секунд. **tries** *number*: указывает количество тайм-аутов последовательных запросов. Если количество тайм-аутов пакетов запросов, передаваемых устройством на тот же сервер безопасности RADIUS, достигает заданного значения, считается, что сервер безопасности RADIUS соответствует условию последовательного тайм-аута недоступности. Значение варьируется от 1 до 100
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если сервер безопасности RADIUS соответствует как условию продолжительности, так и условию тайм-аута последовательных запросов, считается, что сервер безопасности RADIUS недоступен. Пользователи могут использовать эту команду для настройки значений параметров в условии продолжительности и в условии количества тайм-аутов последовательных запросов

Настройка продолжительности прекращения передачи устройством пакетов запросов на недоступный RADIUS-сервер

Команда	**radius-server deadtime** *minutes*
Описание параметров	*minutes*: указывает продолжительность устройство для прекращения передачи запросов на недоступный сервер безопасности RADIUS с

	единицей измерения минут. Значение варьируется от 1 минуты до 1440 минут (24 часа)
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если для сервера безопасности RADIUS на устройстве включена функция активного обнаружения, параметр времени в параметре **radius-server deadtime** не влияет на сервер RADIUS. Если функция активного обнаружения отключена для сервера безопасности RADIUS, устройство автоматически восстанавливает сервер безопасности RADIUS в состояние доступности, когда продолжительность нахождения сервера безопасности RADIUS в недоступном состоянии превышает время, указанное в параметре **radius-server deadtime**

2.4.3.6. Пример конфигурации

Настройка обнаружения доступности на сервере RADIUS

Сценарий:



Рисунок 2-5.

Шаги настройки	• Настройте глобальные критерии для определения того, что сервер безопасности RADIUS недоступен. • Настройте IP-адрес удаленного сервера безопасности RADIUS, порт аутентификации, порт учета и параметры активного обнаружения
RADIUS-клиент	QTECH(config)#radius-server dead-criteria time120 tries 5 QTECH(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
Проверка	Отключите сетевое соединение между устройством и сервером с IP-адресом 192.168.5.22. Проведите аутентификацию RADIUS через устройство. Через 120 секунд запустите команду **show radius server**, чтобы убедиться, что сервер **dead** (не работает)
	QTECH#show running-config … radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90

	radius-server dead-criteria time 120 tries 5 …

2.5. Мониторинг

2.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд очистки может привести к потере жизненно важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает статистику функции расширения динамической авторизации RADIUS и перезапускает статистику	**clear radius dynamic-authorization-extension statistics**

2.5.2. Отображение

Описание	Команда
Отображает глобальные параметры сервера RADIUS	**show radius parameter**
Отображает конфигурацию сервера RADIUS	**show radius server**
Отображает конфигурацию приватного типа атрибута RADIUS	**show radius vendor-specific**
Отображает статистику, относящуюся к функции расширения динамической авторизации RADIUS	**show radius dynamic-authorization-extension statistics**
Отображает статистику, относящуюся к аутентификации RADIUS	**show radius auth statistics**
Отображает статистику, относящуюся к учету RADIUS	**show radius acct statistics**
Отображает конфигурацию групп серверов RADIUS	**show radius group**

2.5.3. Отладка

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

Описание	Команда
Отладка события RADIUS	**debug radius event**
Отладка печати пакетов RADIUS	**debug radius detail**
Отладка функции расширения динамической авторизации RADIUS	**debug radius extension event**
Отладка печати пакетов расширения динамической авторизации RADIUS	**debug radius extension detail**

3. НАСТРОЙКА TACACS+

3.1. Обзор

TACACS+ — это протокол безопасности с расширенными функциями, основанный на протоколе системы управления доступом к контроллеру доступа к терминалу (TACACS). Он используется для реализации аутентификации, авторизации и учета (AAA) нескольких пользователей.

3.1.1. Протоколы и стандарты

RFC 1492 Контроллер доступа к терминалу Системы контроля доступа.

3.2. Приложения

Приложение	Описание
Управление и контроль входа конечных пользователей	Проверка пароля и авторизация должны проводиться для конечных пользователей

3.2.1. Управление и контроль входа конечных пользователей

3.2.1.1. Сценарий

TACACS+ обычно применяется для управления входом в систему и контроля конечных пользователей. Сетевое устройство служит клиентом TACACS+ и отправляет имя пользователя и пароль на сервер TACACS+ для проверки. Пользователю разрешается авторизоваться на сетевом устройстве и выполнять операции после прохождения верификации и получения авторизации. См. следующий Рисунок.

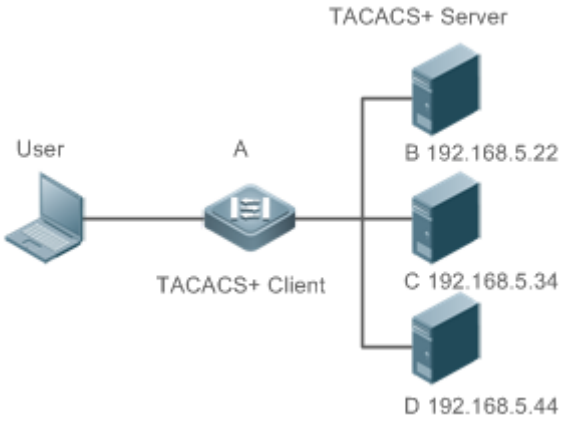


Рисунок 3-1.

A — это клиент, который инициирует запросы TACACS+.

B, C и D — это серверы, обрабатывающие запросы TACACS+.

3.2.1.2. Развертывание

- Запустите сервер TACACS+ на сервере B, сервере C и сервере D и настройте информацию об устройстве доступа (устройство A), чтобы серверы обеспечивали функцию AAA на основе TACACS+ для устройства доступа. Включите функцию AAA на устройстве A, чтобы начать аутентификацию для входа пользователя.

- Включите функцию клиента TACACS+ на устройстве A, добавьте IP-адреса серверов TACACS+ (сервер B, сервер C и сервер D) и совместный ключ, чтобы устройство A связывалось с серверами TACACS+ через TACACS+ для реализации функции AAA.

3.3. Функции

3.3.1. Базовые концепты

Формат пакетов TACACS+

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

Рисунок 3-2.

- Основная версия (Major): указывает основной номер версии TACACS+.
- Второстепенная версия (Minor): указывает второстепенный номер версии TACACS+.
- Тип пакета (Packet Type): указывает тип пакетов, включая следующие параметры: TAC_PLUS_AUTHEN: = 0x01 (аутентификация); TAC_PLUS_AUTHOR:=0x02 (авторизация); TAC_PLUS_ACCT: = 0x03 (учет).
- Порядковый номер (Sequence Number): указывает порядковый номер пакета данных в текущем сеансе. Порядковый номер первого пакета данных TACACS+ в сеансе должен быть равен 1, а порядковый номер каждого последующего пакета данных увеличивается на единицу. Поэтому клиент отправляет пакеты данных только с нечетным порядковым номером, а демон TACACS+ отправляет пакеты только с четным порядковым номером.
- Флаги (Flags): содержит различные флаги растрового формата. Один из битов значения указывает, нужно ли шифровать пакеты данных.
- Идентификатор сеанса (Session ID): указывает идентификатор сеанса TACACS+.
- Длина (Length): указывает длину тела пакета данных TACACS+ (исключая заголовок). Пакеты шифруются для передачи по сети.

3.3.2. Обзор

Особенность	Описание
TACACS+ Аутентификация, авторизация и учет	Выполняет аутентификацию, авторизацию и учет конечных пользователей

3.3.3. TACACS+ Аутентификация, авторизация и учет

3.3.3.1. Принцип работы

На следующем Рисунке используется базовая аутентификация, авторизация и учет входа пользователя для описания взаимодействия пакетов данных TACACS+.

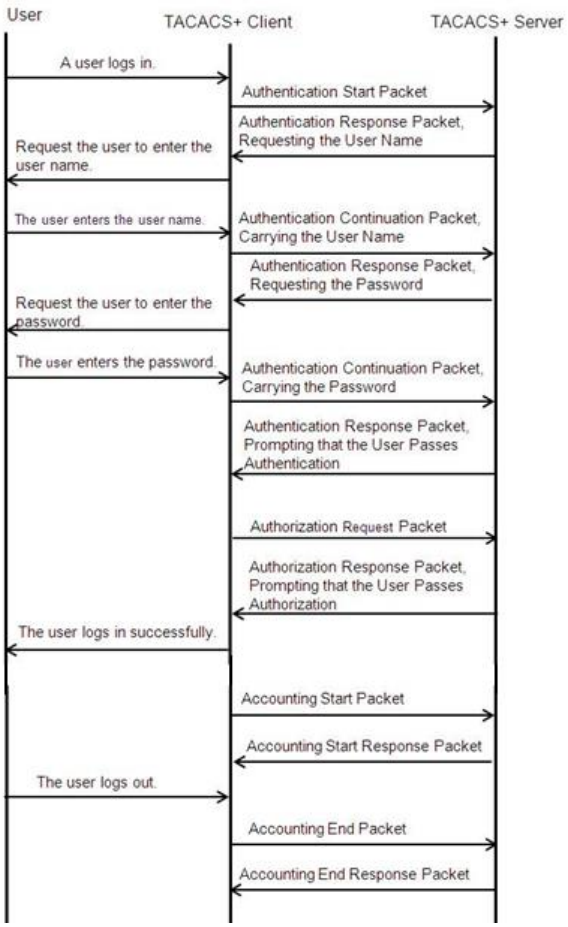


Рисунок 3-3.

Весь базовый процесс взаимодействия с сообщениями включает в себя три секции:

1. Процесс аутентификации описывается следующим образом:
   1.1. Пользователь запрашивает вход на сетевое устройство.
   1.2. После получения запроса клиент TACACS+ отправляет пакет запуска аутентификации на сервер TACACS+.
   1.3. Сервер TACACS+ возвращает пакет ответа аутентификации, запрашивая имя пользователя.
   1.4. Клиент TACACS+ запрашивает пользователя ввести имя пользователя.
   1.5. Пользователь вводит имя пользователя для входа.
   1.6. После получения имени пользователя клиент TACACS+ отправляет пакет продолжения аутентификации, содержащий имя пользователя, на сервер TACACS+.
   1.7. Сервер TACACS+ возвращает ответный пакет идентификации, запрашивая пароль для входа.
   1.8. Клиент TACACS+ запрашивает у пользователя пароль для входа в систему.

1.9. Пользователь вводит пароль для входа.

1.10. После получения пароля для входа клиент TACACS+ отправляет пакет продолжения аутентификации, содержащий пароль для входа на сервер TACACS+.

1.11. Сервер TACACS+ возвращает ответный пакет идентификации, предлагая пользователю пройти аутентификацию.

2. Авторизация пользователя начинается после успешной аутентификации:

2.1. Клиент TACACS+ отправляет пакет запроса авторизации на сервер TACACS+.

2.2. Сервер TACACS+ возвращает ответный пакет авторизации, предлагающий пользователю пройти авторизацию.

2.3. После получения пакета успешной авторизации клиент TACACS+ выводит пользователю экран конфигурации сетевого устройства.

3. Для учета и аудита нужно вести логин пользователя после успешной авторизации:

3.1. Клиент TACACS+ отправляет пакет запуска учета на сервер TACACS+.

3.2. Сервер TACACS+ возвращает ответный пакет учета, сообщая о получении пакета запуска учета.

3.3. Пользователь выходит из системы.

3.4. Клиент TACACS+ отправляет конечный пакет учета на сервер TACACS+.

3.5. Сервер TACACS+ возвращает пакет ответа учета, сообщая о получении конечного пакета учета.

3.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций TACACS+	(Обязательно) Используется для включения службы безопасности TACACS+	
	tacacs-server host	Настраивает сервер TACACS+
	tacacs-server key	указывает ключ, совместно используемый сервером и сетевым устройством
	tacacs-server timeout	Настраивает глобальное время ожидания сервера TACACS+ для связи между сетевым устройством и сервером TACACS+
Настройка раздельной обработки аутентификации, авторизации и учета TACACS+	(Опционально) Он используется для отдельной обработки запросов аутентификации, авторизации и учета	
	aaa group server tacacs+	Настраивает группы серверов TACACS+ и делит серверы TACACS+ на разные группы

Конфигурация	Описание и команда	
Настройка раздельной обработки аутентификации, авторизации и учета TACACS+	**server**	Добавляет серверы в группы серверов TACACS+

3.4.1. Настройка основных функций TACACS+

3.4.1.1. Эффект конфигурации

- Основные функции TACACS+ доступны после завершения настройки. При настройке списка методов AAA укажите метод использования TACACS+ для реализации аутентификации, авторизации и учета TACACS+.
- Когда выполняются операции аутентификации, авторизации и учета, TACACS+ инициирует запросы аутентификации, авторизации и учета к настроенным серверам TACACS+ в соответствии с настроенной последовательностью. Если время ожидания ответа истекло на сервере TACACS+, TACACS+ последовательно просматривает список серверов TACACS+.

3.4.1.2. Примечания

- Служба безопасности TACACS+ относится к типу службы AAA. Вам нужно запустить команду **aaa new-model**, чтобы включить службу безопасности.
- После настройки основных функций TACACS+ предоставляется только одна служба безопасности. Чтобы функции TACACS+ работали, укажите службу TACACS+ при настройке списка методов AAA.

3.4.1.3. Шаги настройки

Включение AAA

Обязательный. Список методов AAA можно настроить только после включения AAA. TACACS+ предоставляет услуги в соответствии со списком методов AAA.

Команда	**aaa new-model**
По умолчанию	Функция AAA отключена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Список методов AAA можно настроить только после включения AAA. TACACS+ предоставляет услуги в соответствии со списком методов AAA

Настройка IP-адреса сервера TACACS+

Обязательный. В противном случае устройство не сможет связаться с сервером TACACS+ для реализации функции AAA.

Команда	**tacacs-server host** [**oob**] [**via** *mgmt_name*] *ipv4-address* [**port** *integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]
Описание параметров	*ipv4-address*: указывает IPv4-адрес сервера TACACS+. **oob**: использует порт MGMT в качестве исходного интерфейса для связи с сервером TACACS+. Не порт MGMT используется для связи по умолчанию. **via** *mgmt_name*: указывает конкретный порт MGMT, когда oob поддерживает несколько портов MGMT. **port** *integer*: указывает порт TCP, используемый для связи TACACS+. TCP-порт по умолчанию — 49. **timeout** *integer*: указывает время ожидания связи с сервером TACACS+. Глобальное время ожидания используется по умолчанию. **key** [**0** | **7**] *text-string*: указывает совместный ключ сервера. Глобальный ключ используется, если он не настроен. Для сконфигурированного ключа можно указать тип шифрования. Значение 0 указывает на отсутствие шифрования, а 7 указывает на простое шифрование. Значение по умолчанию — 0
По умолчанию	Сервер TACACS+ не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Вы можете указать совместный ключ сервера при настройке IP-адреса сервера. Если совместный ключ не указан, в качестве общего ключа сервера используется глобальный ключ, настроенный с помощью команды **tacacs-server key**. Совместный ключ должен быть полностью таким же, как настроенный на сервере. Вы можете указать коммуникационный порт сервера при настройке IP-адреса. Время ожидания связи сервера можно указать при настройке IP-адреса

Настройка общего ключа сервера TACACS+

- Опционально.
- Если с помощью этой команды не настроен глобальный коммуникационный протокол, установите ключ, чтобы указать совместный ключ сервера при выполнении команды **tacacs-server host** для добавления информации о сервере. В противном случае устройство не сможет связаться с сервером TACACS+.
- Если совместный ключ не указан с помощью **key** при запуске команды **tacacs-server host** для добавления информации о сервере, используется глобальный ключ.

Команда	**tacacs-server** [**key** [**0** | **7**] *text-string*]
Описание параметров	*text-string*: указывает текст общего ключа. **0 | 7**: указывает тип шифрования ключа. Значение 0 указывает на отсутствие шифрования, а 7 указывает на простое шифрование
По умолчанию	Совместный ключ не настроен ни для одного сервера TACACS+
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки глобального общего ключа для серверов. Чтобы указать разные ключи для каждого сервера, установите ключ при выполнении команды **tacacs-server host**

Настройка времени ожидания (тайм-аута) сервера TACACS+

- Опционально.
- Вы можете установить тайм-аут на большое значение, когда связь между устройством и сервером нестабильна.

Команда	**tacacs-server timeout** *seconds*
Описание параметров	*seconds*: указывает время ожидания в секундах. Значение варьируется от 1 секунды до 1000 секунд
По умолчанию	Значение по умолчанию — 5 секунд
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки глобального тайм-аута ответа сервера. Чтобы установить разное время ожидания для каждого сервера, установите время ожидания при выполнении команды **tacacs-server host**

3.4.1.4. Проверка

Настройте список методов AAA, указывающий на выполнение аутентификации, авторизации и учета пользователей с помощью TACACS+.

- Включите взаимодействие устройства с сервером TACACS+ и выполните захват пакетов, чтобы проверить процесс взаимодействия TACACS+ между устройством и сервером TACACS+.
- Просмотрите журналы сервера, чтобы проверить, нормально ли работают аутентификация, авторизация и учет.

3.4.1.5. Пример конфигурации

Использование TACACS+ для аутентификации при входе

Сценарий:



Рисунок 3-4.

A — это клиент, который инициирует запросы TACACS+.

B — это сервер, который обрабатывает запросы TACACS+.

Шаги настройки	• Включить AAA. • Настройте информацию о сервере TACACS+. • Настройте метод использования TACACS+ для аутентификации. • Примените настроенный метод идентификации на интерфейсе
A	QTECH# configure terminal QTECH(config)# aaa new-model QTECH(config)# tacacs-server host 192.168.5.22 QTECH(config)# tacacs-server key aaa QTECH(config)# aaa authentication login test group tacacs+ QTECH(config)# line vty 0 4 QTECH(config-line)# login authentication test
Проверка	Telnet к устройству с ПК. Отображается экран с запросом имени пользователя и пароля. Введите правильное имя пользователя и пароль для входа в устройство. Просмотрите журнал аутентификации пользователя на сервере TACACS+

3.4.1.6. Распространенные ошибки

- Служба безопасности AAA отключена.
- Ключ, настроенный на устройстве, не соответствует ключу, настроенному на сервере.
- Список методов не настроен.

3.4.2. Настройка раздельной обработки аутентификации, авторизации и учета TACACS+

3.4.2.1. Эффект конфигурации

Аутентификация, авторизация и учет в службе безопасности обрабатываются разными серверами TACACS+, что повышает безопасность и в определенной степени обеспечивает балансировку нагрузки.

3.4.2.2. Примечания

- Служба безопасности TACACS+ относится к типу службы AAA. Вам нужно запустить команду **aaa new-model**, чтобы включить службу безопасности.
- После настройки основных функций TACACS+ предоставляется только одна служба безопасности. Чтобы функции TACACS+ работали, укажите службу TACACS+ при настройке списка методов AAA.

3.4.2.3. Шаги настройки

Настройка групп серверов TACACS+

- Обязательный. По умолчанию существует только одна группа серверов TACACS+, которая не может реализовать отдельную обработку аутентификации, авторизации и учета.
- Необходимо настроить три группы серверов TACACS+ для отдельной обработки аутентификации, авторизации и учета.

Команда	**aaa group server tacacs+***group-name*
Описание параметров	*group-name*: указывает имя группы. Имя группы не может быть radius или tacacs+, которые являются именами встроенных групп
По умолчанию	Группа серверов TACACS+ не настроена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Сгруппируйте серверы TACACS+, чтобы аутентификация, авторизация и учет выполнялись разными группами серверов

Добавление серверов в группы серверов TACACS+

- Обязательный. Если сервер не добавлен в группу серверов, устройство не может обмениваться данными с серверами TACACS+.
- В режиме конфигурации группы серверов добавьте серверы, настроенные с помощью команды **tacacs-server host**.

Команда	**server** *ipv4-address*
Описание параметров	*ipv4-address*: указывает IPv4-адрес сервера TACACS+

По умолчанию	Ни один сервер не настроен
Командный режим	Режим конфигурации группы серверов TACACS+
Руководство по использованию	Перед настройкой этой команды необходимо запустить команду **aaa group server tacacs+**, чтобы войти в режим конфигурации группы серверов TACACS+. Для адреса сервера, настроенного в группе серверов TACACS+, сервер должен быть настроен с помощью команды **tacacs-server host** в режиме глобальной конфигурации. Если в одну группу серверов добавлено несколько серверов, когда один сервер не отвечает, устройство продолжает отправлять запрос TACACS+ на другой сервер в группе серверов

Настройка VRF группы серверов TACACS+

- Опционально. Настройте виртуальную маршрутизацию и пересылку (VRF), если устройству необходимо отправлять пакеты TACACS+ через указанный адрес.
- В режиме конфигурации группы серверов используйте настроенное имя VRF, чтобы указать маршрут для связи серверов в этой группе.

Команда	**ip vrf forwarding** *vrf-name*
Описание параметров	*vrf-name*: указывает имя VRF
По умолчанию	По умолчанию VRF не указан
Командный режим	Режим конфигурации группы серверов TACACS+
Руководство по использованию	Перед настройкой этой команды необходимо запустить команду **aaa group server tacacs+**, чтобы войти в режим конфигурации группы серверов TACACS+. Для VRF, настроенного в группе серверов TACACS+, допустимое имя должно быть настроено для VRF с помощью команды **vrf definition** в режиме глобальной конфигурации

Настройка oob группы серверов TACACS+

- Опционально. Настройте oob, если устройству необходимо отправлять пакеты TACACS+ через указанный порт MGMT.
- В режиме конфигурации группы серверов укажите маршрутизацию для связи серверов в группе.

Команда	**ip oob via** *mgmt_name*
Описание параметров	*mgmt_name*: указывает имя порта управления
По умолчанию	По умолчанию oob не указан
Командный режим	Режим конфигурации группы серверов TACACS+
Руководство по использованию	Перед настройкой этой команды необходимо запустить команду **aaa group server tacacs+**, чтобы войти в режим конфигурации группы серверов TACACS+. Если порт MGMT не указан, по умолчанию используется порт MGMT0

3.4.2.4. Проверка

- Настройте список методов AAA, указывающий на выполнение аутентификации, авторизации и учета пользователей с помощью TACACS+.
- Включите взаимодействие устройства с серверами TACACS+. Выполните захват пакетов, убедитесь, что пакеты аутентификации, авторизации и учета взаимодействуют с разными серверами, и проверьте исходные адреса в пакетах.

3.4.2.5. Пример конфигурации

Настройка различных групп серверов TACACS+ для отдельной обработки аутентификации, авторизации и учета

Сценарий:

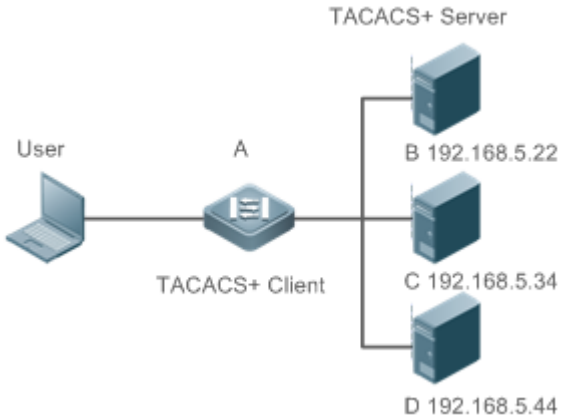


Рисунок 3-5.

A — это клиент, который инициирует запросы TACACS+.

B — это сервер, который обрабатывает запросы аутентификации TACACS+.

C — это сервер, который обрабатывает запросы авторизации TACACS+.

D — это сервер, который обрабатывает учетные запросы TACACS+.

Шаги настройки	• Включить AAA. • Настройте информацию о сервере TACACS+. • Настройте группы серверов TACACS+. • Добавьте серверы в группы серверов TACACS+. • Настройте метод использования TACACS+ для аутентификации. • Настройте метод использования TACACS+ для авторизации. • Настройте метод использования TACACS+ для учета. • Примените настроенный метод идентификации на интерфейсе. • Примените настроенный метод авторизации на интерфейсе. • Примените настроенный метод учета на интерфейсе
	QTECH# configure terminal QTECH(QTECH(config)# aaa new-model QTECH(config)# tacacs-server host 192.168.5.22 QTECH(config)# tacacs-server host 192.168.5.34 QTECH(config)# tacacs-server host 192.168.5.44 QTECH(config)# tacacs-server key aaa QTECH(config)# aaa group server tacacs+ tacgrp1 QTECH(config-gs-tacacs)# server 192.168.5.22 QTECH(config-gs-tacacs)# exit QTECH(config)# aaa group server tacacs+ tacgrp2 QTECH(config-gs-tacacs)# server 192.168.5.34 QTECH(config-gs-tacacs)# exit QTECH(config)# aaa group server tacacs+ tacgrp3 QTECH(config-gs-tacacs)# server 192.168.5.44 QTECH(config-gs-tacacs)# exit QTECH(config)# aaa authentication login test1 group tacacs+ QTECH(config)# aaa authentication enable default group tacgrp1 QTECH(config)# aaa authorization exec test2 group tacgrp2 QTECH(config)# aaa accounting commands 15 test3 start-stop group tacgrp3 QTECH(config)# line vty 0 4 QTECH(config-line)# login authentication test1 QTECH(config-line)#authorization exec test2 QTECH(config-line)# accounting commands 15 test3
Проверка	Telnet к устройству с ПК. Отображается экран с запросом имени пользователя и пароля. Введите правильное имя пользователя и пароль для входа в устройство. Введите команду enable и введите правильный пароль enable, чтобы инициировать аутентификацию enable. Войдите в

	привилегированный режим EXEC после прохождения аутентификации. Выполните операции на устройстве, а затем выйдите из устройства. Просмотрите журнал аутентификации пользователя на сервере с IP-адресом 192.168.5.22. Просмотрите журнал включения аутентификации пользователя на сервере с IP-адресом 192.168.5.22. Просмотрите журнал авторизации exec пользователя на сервере с IP-адресом 192.168.5.34. Посмотреть журнал учета команд пользователя на сервере с IP-адресом 192.168.5.44

3.4.2.6. Распространенные ошибки

- Служба безопасности AAA отключена.
- Ключ, настроенный на устройстве, не соответствует ключу, настроенному на сервере.
- Неопределенные серверы добавляются в группу серверов.
- Список методов не настроен.

3.5. Мониторинг

3.5.1. Отображение

Описание	Команда
Отображает взаимодействие с каждым сервером TACACS+	**show tacacs**

3.5.2. Отладка

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

Описание	Команда
Отладка TACACS+	**debug tacacs+**

4. КОНФИГУРАЦИЯ SCC

4.1. Обзор

Центр управления безопасностью (SCC) предоставляет общие методы настройки и интеграцию политик для различных служб управления доступом и безопасности сети, так что эти службы управления доступом и безопасности сети могут сосуществовать на одном устройстве для удовлетворения разнообразных требований к управлению доступом и безопасностью в различных сценариях.

Службы сетевой безопасности включают в себя список управления доступом (ACL), политику сетевой защиты (NFPP) и защиту от спуфинга шлюза ARP. Когда на устройстве одновременно включены две или более служб управления доступом или сетевой безопасности, или, когда на устройстве одновременно включены и службы управления доступом, и службы сетевой безопасности, SCC координирует сосуществование этих служб в соответствии с соответствующими политиками.

ПРИМЕЧАНИЕ: дополнительные сведения о службах контроля доступа и безопасности сети см. в соответствующем руководстве по настройке. В этом документе описывается только SCC.

4.2. Приложение

Типичное применение	Сценарий
Контроль доступа к расширенным кампусным сетям уровня 2	Студенты в сети кампуса могут получить доступ к Интернету на основе аутентификации клиента dot1x или веб-аутентификации. Подмена ARP между учащимися должна быть предотвращена. Кроме того, терминальные устройства в некоторых отделах (например, в кабинете директора) могут выходить в Интернет без аутентификации

4.2.1. Контроль доступа к расширенным кампусным сетям уровня 2

4.2.1.1. Сценарий

Студенты в сети кампуса университета обычно должны пройти аутентификацию через клиента dot1x или веб-сайт перед доступом в Интернет, чтобы облегчить учет и гарантировать преимущества университета.

- Учащиеся могут получить доступ к Интернету с помощью клиентской аутентификации dot1x или веб-аутентификации.
- Подмена ARP между студентами предотвращается, чтобы гарантировать стабильность сети.
- Терминальные устройства в некоторых отделах (например, в кабинете директора) могут выходить в Интернет без аутентификации.

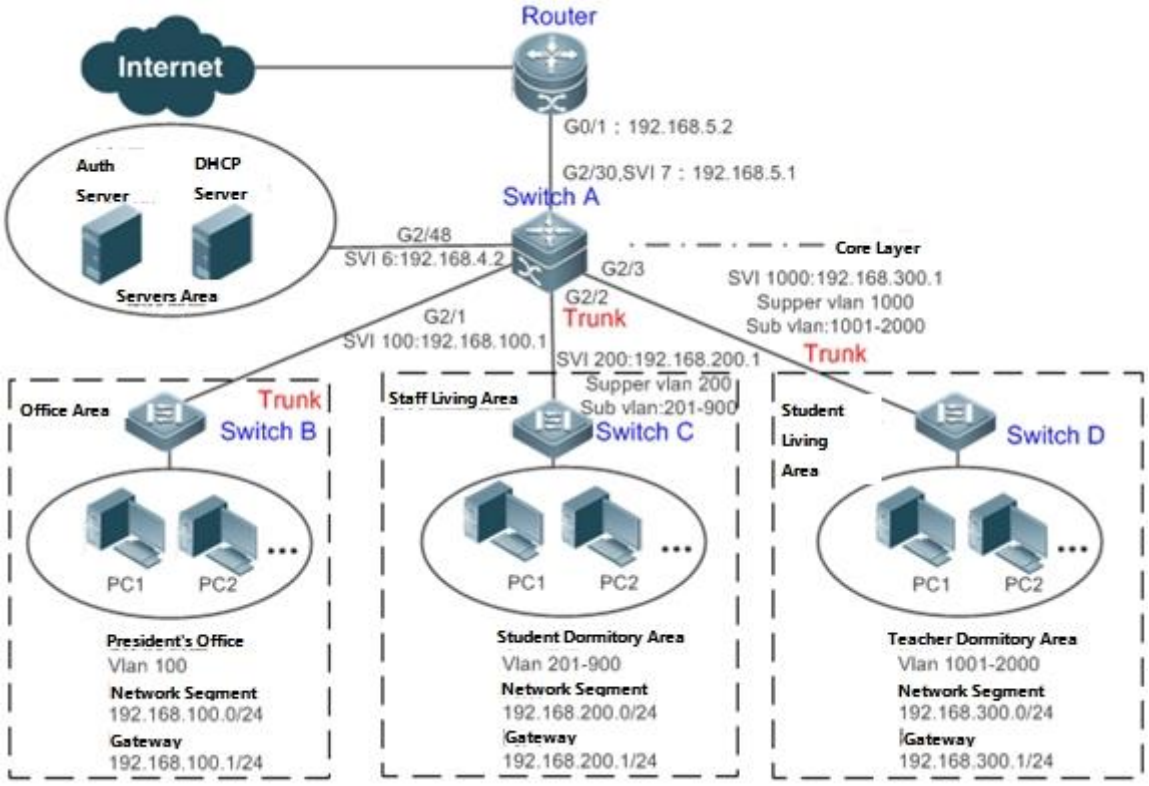


Рисунок 4-1.

Традиционная кампусная сеть спроектирована иерархически и состоит из уровня доступа, уровня конвергенции и уровня ядра, где уровень доступа выполняет управление доступом пользователей. Однако в расширенной кампусной сети уровня 2 управление доступом пользователей осуществляется с помощью коммутатора ядра, ниже которого существуют коммутаторы доступа без участия какого-либо промежуточного устройства. Все порты между коммутатором ядра и коммутаторами доступа (такими как коммутаторы B, C и D на Рисунке 4-1) являются транковыми портами.

Коммутаторы пользовательского доступа B, C и D подключаются к ПК в различных отделах через порты доступа, а виртуальные локальные сети соответствуют вложенным виртуальным локальным сетям, настроенным на нисходящих портах коммутатора ядра, поэтому пользователи доступа находятся в разных виртуальных локальных сетях для предотвращения спуфинга ARP.

Коммутатор ядра A подключается к различным серверам, таким как сервер аутентификации и сервер DHCP. Супер-VLAN и sub VLAN настраиваются на нисходящих портах. Одна супер-VLAN соответствует нескольким sub VLAN, и каждая sub VLAN предоставляет пользователям доступ.

4.2.1.2. Развертывание

На коммутаторе ядра разные пользователи доступа идентифицируются по VLAN и номерам портов. Каждый пользователь доступа (или группа пользователей доступа) соответствует одной VLAN. Порты на каждом коммутаторе доступа, которые подключаются к нижестоящим пользователям, настраиваются как порты доступа, и каждому пользователю доступа назначается одна пользовательская VLAN в соответствии с планированием VLAN. Коммутатор ядра не пересылает запросы ARP. Коммутатор ядра отвечает на запросы ARP только от аутентифицированных пользователей, чтобы предотвратить спуфинг ARP. На коммутаторе ядра A пользовательские VLAN

рассматриваются как sub VLAN, супер-VLAN настраиваются, а SVI, соответствующие супер-VLAN, настраиваются как пользовательские шлюзы.

- На downlink-портах коммутатора ядра (коммутатор A в этом примере), которые подключаются к жилой зоне учителя и жилой зоне учащихся, включены как аутентификация dot1x, так и веб-аутентификация, поэтому пользователи могут свободно выбирать любой режим аутентификации для доступа в Интернет.
- Любой специальный отдел (такой как кабинет директора в этом примере) может быть выделен для конкретной VLAN, и эта VLAN может быть настроена как VLAN без аутентификации, чтобы пользователи в этом отделе могли выходить в Интернет без аутентификации.

4.2.1.3. Базовые концепты

Режим аутентификации

Существует два режима аутентификации: аутентификация доступа и аутентификация шлюза. В традиционной иерархической сети аутентификация доступа обычно выполняется коммутаторами доступа. В расширенной сети уровня 2 функция доступа передается коммутатору ядра, в то время как устройства доступа должны поддерживать только базовые функции переадресации VLAN и уровня 2. Поскольку аутентификация доступа выполняется коммутаторами доступа в традиционной иерархической сети, а коммутатором ядра — в расширенной многослойной сети уровня 2, некоторые внешние функции и поведение будут различаться соответственно для двух разных режимов аутентификации. Таким образом, режим аутентификации относится к аутентификации шлюза и аутентификации доступа. Если аутентификация доступа перемещается на коммутатор ядра, коммутатор ядра должен быть включен с режимом аутентификации шлюза для поддержки большого количества пользовательских записей, обычно включая таблицу MAC-адресов большой емкости, таблицу ARP и таблицу маршрутизации. В противном случае количество поддерживаемых пользователей зависит от аппаратных ограничений на записи ACL. Как правило, емкость аппаратных записей ACL ограничена и не может поддерживать большое количество пользователей. Режим аутентификации доступа обычно применим только в сценариях, где аутентификация доступа развернута на коммутаторах доступа.

VLAN с освобождением от аутентификации

Некоторые специальные отделы могут быть выделены для VLAN без аутентификации, чтобы упростить управление сетью, чтобы пользователи в этих отделах могли получать доступ к сетевым ресурсам без аутентификации. Например, кабинет директора можно разделить на виртуальные локальные сети без аутентификации в сети кампуса, чтобы пользователи в кабинете директора могли выходить в Интернет без аутентификации.

Количество пользователей IPv4

Количество пользователей доступа IPv4 может быть ограничено, чтобы защитить стабильность доступа онлайн-пользователей в Интернете и улучшить стабильность работы устройства.

ПРИМЕЧАНИЕ: количество пользователей доступа IPv4 по умолчанию не ограничено; то есть большое количество пользователей может выйти в сеть после аутентификации, пока не будет достигнута максимальная аппаратная мощность устройства.

Миграция аутентифицированных пользователей

Миграция онлайн-пользователя означает, что онлайн-пользователь может снова пройти аутентификацию из разных физических местоположений для доступа к сети. Однако в сети кампуса для простоты управления студентам обычно предлагается пройти аутентификацию из определенного места перед доступом в Интернет, но они не могут

пройти аутентификацию на других портах доступа. Это означает, что пользователи не могут мигрировать. В другом случае у некоторых пользователей есть требование мобильного офиса, и они могут проходить аутентификацию из разных мест доступа. Затем пользователи могут мигрировать.

4.2.1.4. Функции

Особенность	Функция
Режим аутентификации	Эта функция определяет, развертывается ли управление доступом на коммутаторах доступа или коммутаторах ядра в зависимости от потребностей развертывания сети
VLAN с освобождением от аутентификации	Пользователи в указанной VLAN могут быть настроены как пользователи с освобождением от аутентификации
Количество пользователей IPv4	Пользовательская емкость IPv4 указанного интерфейса может быть ограничена, чтобы гарантировать стабильность доступа пользователей в Интернете
Миграция аутентифицированных пользователей	Вы можете указать, могут ли аутентифицированные пользователи мигрировать
Обнаружение онлайн-статуса пользователя	Вы можете указать, следует ли обнаруживать трафик онлайн-пользователей, чтобы пользователь отключался от сети, когда трафик пользователя ниже заданного значения в течение определенного периода времени

4.2.2. Режим аутентификации

Существует два режима аутентификации: аутентификация доступа и аутентификация шлюза. В режиме аутентификации доступа управление доступом включено на коммутаторах доступа. В режиме аутентификации шлюза управление доступом включено на коммутаторах ядра. В крупномасштабной сети, такой как кампусная сеть, есть сотни коммутаторов доступа. По сравнению с режимом аутентификации доступа режим аутентификации шлюза упрощает рутинное обслуживание и управление коммутаторами доступа, поскольку коммутаторы доступа должны поддерживать только основные функции переадресации VLAN и уровня 2. Поэтому рекомендуется режим аутентификации шлюза.

4.2.2.1. Принцип работы

Режим аутентификации на устройстве зависит от сетевого уровня, на котором работает устройство управления доступом. Если управление доступом развернуто на коммутаторах ядра (например, в расширенной сети уровня 2), требуется режим аутентификации шлюза на коммутаторах ядра. Если управление доступом развернуто на коммутаторах доступа, режим аутентификации должен быть установлен на аутентификацию доступа на коммутаторах доступа.

ПРИМЕЧАНИЕ: перезагрузите устройство после изменения режима аутентификации, чтобы новый режим аутентификации вступил в силу. Сохраните текущую конфигурацию перед перезапуском устройства.

4.2.3. VLAN с освобождением от аутентификации

Виртуальные локальные сети с освобождением от идентификации используются для размещения отделов с особыми требованиями к доступу, чтобы пользователи этих отделов могли выходить в Интернет без идентификации, такой как dot1x или веб-аутентификация.

4.2.3.1. Принцип работы

Предположим, что на устройстве включена функция VLAN с освобождением от аутентификации. Когда устройство обнаруживает, что пакет поступает из сети VLAN без идентификации, управление доступом не выполняется. Таким образом, пользователи VLAN без идентификации могут получить доступ к Интернету без идентификации. Функцию VLAN с освобождением от аутентификации можно рассматривать как разновидность приложений защищенных каналов.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают функцию VLAN с освобождением от аутентификации.

ПРИМЕЧАНИЕ: можно настроить до 100 VLAN с освобождением от аутентификации.

ПРИМЕЧАНИЕ: VLAN с освобождением от аутентификации занимают аппаратные записи. Когда управление доступом, такое как аутентификация, отключено, настройка VLAN с освобождением от аутентификации имеет тот же эффект, что и в случае, когда VLAN с освобождением от аутентификации не настроены. Поэтому рекомендуется настраивать виртуальные локальные сети без аутентификации для пользователей, которым требуется доступ в Интернет без аутентификации, только при включенной функции управления доступом.

ПРИМЕЧАНИЕ: хотя пакеты из сетей VLAN с освобождением от аутентификации освобождены от контроля доступа, они все равно должны быть проверены с помощью security ACL. Если пакеты пользователей в VLAN без аутентификации отклонены в соответствии с security ACL, пользователи все равно не могут получить доступ к Интернету.

ПРИМЕЧАНИЕ: в режиме аутентификации шлюза устройство не инициирует никаких ARP-запросов к пользователю в VLAN без аутентификации, и прокси-сервер ARP не будет работать. Таким образом, в режиме аутентификации шлюза пользователи в разных сетях VLAN, освобожденных от аутентификации, не могут получить доступ друг к другу до тех пор, пока пользователи не будут аутентифицированы.

4.2.4. Количество пользователей IPv4

Для повышения стабильности работы устройства и защиты от грубого силового воздействия со стороны неавторизованных пользователей вы можете ограничить общее количество пользователей доступа IPv4 на определенном порту устройства.

4.2.4.1. Принцип работы

Если общее количество пользователей с доступом к IPv4 ограничено, новые пользователи, превышающие общее количество, не могут получить доступ к Интернету.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают ограничение на количество пользователей доступа IPv4.

ПРИМЕЧАНИЕ: количество пользователей доступа IPv4 не ограничено на устройстве по умолчанию, но зависит от аппаратных возможностей устройства.

ПРИМЕЧАНИЕ: в число пользователей доступа IPv4 входят пользователи IPv4 на основе различных функций привязки. Поскольку количество пользователей доступа IPv4

настраивается в режиме конфигурации интерфейса, ограничение включает как количество пользователей IPv4, сгенерированных на порту, так и глобально сгенерированных пользователей IPv4. Например, вы можете установить максимальное количество пользователей доступа IPv4 на порту Gi 0/1 равным 2, запустить команды для привязки пользователя IPv4 к порту, а затем запустить команды для привязки глобального пользователя IPv4 к порту. На самом деле на порту уже есть два пользователя доступа. Если вы попытаетесь привязать другого пользователя IPv4 или другого глобального пользователя IPv4 к порту, операция привязки завершится ошибкой.

4.2.5. Миграция аутентифицированных пользователей

В реальной сети пользователи не обязательно получают доступ к Интернету из фиксированного места. Вместо этого пользователи могут быть переведены в другой отдел или офис после прохождения аутентификации в одном месте. Они не отключаются активно, а отключают сетевые кабели и переносят свои мобильные терминалы в новый офис для доступа к сети. Затем это приводит к проблеме миграции аутентифицированных пользователей. Если миграция пользователей, прошедших аутентификацию, не настроена, пользователь, подключающийся к сети в одном месте, не может подключиться к сети в другом месте без предварительного выхода в автономный режим.

4.2.5.1. Принцип работы

Когда миграция аутентифицированных пользователей включена, модуль dot1x или веб-аутентификации устройства обнаруживает, что номер порта или VLAN, соответствующий MAC-адресу пользователя, изменился. Затем пользователь принудительно отключается от сети и должен снова пройти аутентификацию, прежде чем подключаться к сети.

ПРИМЕЧАНИЕ: функция миграции аутентифицированных пользователей требует проверки MAC-адресов пользователей и недействительна для пользователей, у которых есть только IP-адреса.

ПРИМЕЧАНИЕ: функция миграции пользователей, прошедших аутентификацию, позволяет пользователю, который подключается к сети в одном месте, подключаться к сети в другом месте, не отключаясь сначала. Если пользователь подключается к сети в одном месте, а затем выходит из сети в этом месте, или если пользователь не подключается к сети до перехода в другое место, ситуация выходит за рамки диапазона миграции аутентифицированных пользователей.

ПРИМЕЧАНИЕ: во время миграции система проверяет, изменился ли идентификатор VLAN или номер порта, соответствующий MAC-адресу пользователя, чтобы определить, мигрировал ли пользователь. Если идентификатор VLAN или номер порта совпадают, это означает, что пользователь не мигрирует; в противном случае это означает, что пользователь мигрировал. В соответствии с предыдущим принципом, если другой пользователь в сети использует MAC-адрес онлайн-пользователя, система ошибочно отключит онлайн-пользователя, если не будет принято дополнительное решение. Чтобы предотвратить такую проблему, dot1x или веб-аутентификация проверят, действительно ли пользователь мигрировал. Для пользователя, который подключается к сети через веб-аутентификацию или аутентификацию dot1x с авторизацией по IP, dot1x или веб-аутентификация отправляет запрос ARP в исходное место пользователя, если обнаруживает, что тот же MAC-адрес находится в сети в другой VLAN или на другом порту. Если в течение указанного времени ответ не получен, это означает, что местоположение пользователя действительно изменилось, и миграция разрешена. Если ответ получен в течение указанного времени, это указывает на то, что пользователь фактически не мигрирует и в сети может существовать мошеннический пользователь. В последнем случае миграция не выполняется. Запрос ARP отправляется раз в секунду по умолчанию

и отправляется в общей сложности пять раз. Это означает, что миграция может быть подтверждена только через пять секунд. Параметры, связанные с тайм-аутом, включая интервал и время проверки, можно изменить с помощью команд **arp retry times** *times* и **arp retry interval** *interval*.

4.2.6. Обнаружение онлайн-статуса пользователя

После того, как пользователь выходит в Интернет, он может забыть выйти в автономный режим или не может выйти в автономный режим из-за сбоев терминала. В этом случае с пользователя будет продолжать взиматься плата, и поэтому он понесет определенные экономические потери. Чтобы защитить преимущества пользователей в Интернете, в устройстве предусмотрена функция определения того, действительно ли пользователи находятся в сети. Если устройство считает, что пользователь не в сети, оно активно отключает пользователя.

4.2.6.1. Принцип работы

Определенный интервал обнаружения предустановлен на устройстве. Если трафик пользователя ниже определенного значения в этом интервале, устройство считает, что пользователь не использует сеть, и поэтому напрямую отключает пользователя.

4.3. Конфигурация

Элемент конфигурации	Предложения и связанные с ними команды	
Настройка режима аутентификации	Необязательная конфигурация, которая используется для настройки режима аутентификации для устройства	
	[no] auth-mode gateway	Настраивает режим аутентификации
Настройка VLAN с освобождением от аутентификации	Необязательная конфигурация, которая используется для указания пользователей, чьи VLAN могут выходить в Интернет без аутентификации	
	[no] direct-vlan	Настраивает VLAN без аутентификации
Настройка количества пользователей IPv4	Необязательная конфигурация, которая используется для указания максимального количества пользователей, которым разрешен доступ к определенному интерфейсу	
	[no] nac-author-user maximum	Настраивает количество пользователей IPv4, которым разрешен доступ к определенному интерфейсу

Элемент конфигурации	Предложения и связанные с ними команды	
Настройка миграции авторизованных пользователей	Необязательная конфигурация, которая используется, чтобы указать, могут ли онлайн-пользователи со статическими MAC-адресами мигрировать	
	[no] station-move permit	Настраивает, могут ли пользователи, прошедшие аутентификацию, мигрировать
Настройка определения онлайн-статуса пользователя	Необязательная конфигурация, которая используется для указания, следует ли включать функцию определения онлайн-статуса пользователя	
	offline-detect interval threshold	Настраивает параметры функции определения онлайн-статуса пользователя
	no offline-detect	Отключает функцию определения онлайн-статуса пользователя
	default offline-detect	Восстанавливает режим определения онлайн-статуса пользователя по умолчанию

4.3.1. Настройка режима аутентификации

4.3.1.1. Эффект конфигурации

Выполнять эту настройку или не выполнять эту настройку, что зависит от фактического развертывания сети. В иерархической сети коммутаторы доступа выполняют управление доступом, и вам не нужно указывать режим аутентификации, вы можете просто сохранить конфигурацию по умолчанию. В расширенной сети уровня 2 с удаленным уровнем доступа устройство шлюза выполняет управление доступом, а затем вам необходимо установить режим аутентификации на аутентификацию шлюза, чтобы пользователи могли пройти аутентификацию и подключиться к сети после того как служба управления доступом, такая как dot1x или веб-аутентификация, включена на шлюзовом устройстве.

4.3.1.2. Меры предосторожности

- Если управление доступом развернуто на коммутаторе ядра, вам необходимо изменить режим аутентификации на коммутаторе ядра на аутентификацию шлюза. Если контроль доступа не развернут на коммутаторе ядра, вам не нужно настраивать режим аутентификации.
- Вам необходимо перезагрузить устройство после изменения режима аутентификации, чтобы новый режим аутентификации вступил в силу. Сохраните текущую конфигурацию перед перезапуском устройства.

4.3.1.3. Метод конфигурации

Настройка режима аутентификации

- Дополнительная конфигурация. Он определяет позицию доступа устройства в реальной сети.
- Выполните настройку в соответствии с фактическим развертыванием сети. Если коммутатор ядра выполняет управление доступом, установите режим аутентификации на аутентификацию шлюза на коммутаторе ядра; в противном случае просто оставьте конфигурацию по умолчанию.

Команда	**[no] auth-mode gateway**
Описание параметров	**no**: если команда содержит этот параметр, это указывает, что режим аутентификации восстановлен для аутентификации доступа; то есть локальное устройство является только устройством доступа, а не шлюзовым устройством. **auth-mode gateway**: если команда содержит этот параметр, это указывает, что режим аутентификации установлен на аутентификацию шлюза; то есть локальное устройство является одновременно устройством шлюза и устройством доступа
По умолчанию	Режим аутентификации доступа
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы определить позицию доступа устройства в сети. Выполнять эту настройку или не выполнять эту настройку, что зависит от того, развернута ли функция управления доступом на коммутаторах доступа в сети или развернута на устройстве шлюза. Используйте эту команду, чтобы изменить режим аутентификации, настроенный на устройстве, с аутентификации доступа на аутентификацию шлюза. Используйте команду **no auth-mode gateway**, чтобы изменить режим аутентификации, настроенный на устройстве, с аутентификации шлюза обратно на аутентификацию доступа

4.3.1.4. Проверка

ПРИМЕЧАНИЕ: проверьте конфигурацию, используя следующий метод:

Включите dot1x или веб-аутентификацию на одном порту устройства и выполните соответствующую аутентификацию на клиенте. После подключения к Интернету проверьте, можете ли вы получить доступ к сетевым ресурсам. Затем отключитесь и проверьте, не можете ли вы получить доступ к указанным сетевым ресурсам.

4.3.1.5. Примеры конфигурации

В следующем примере конфигурации описывается только конфигурация, связанная с SCC.

Установка режима аутентификации на аутентификацию шлюза, чтобы функция управления доступом переместилась на шлюзовое устройство ядра в расширенной сети уровня 2 с удаленным уровнем

Сценарий:

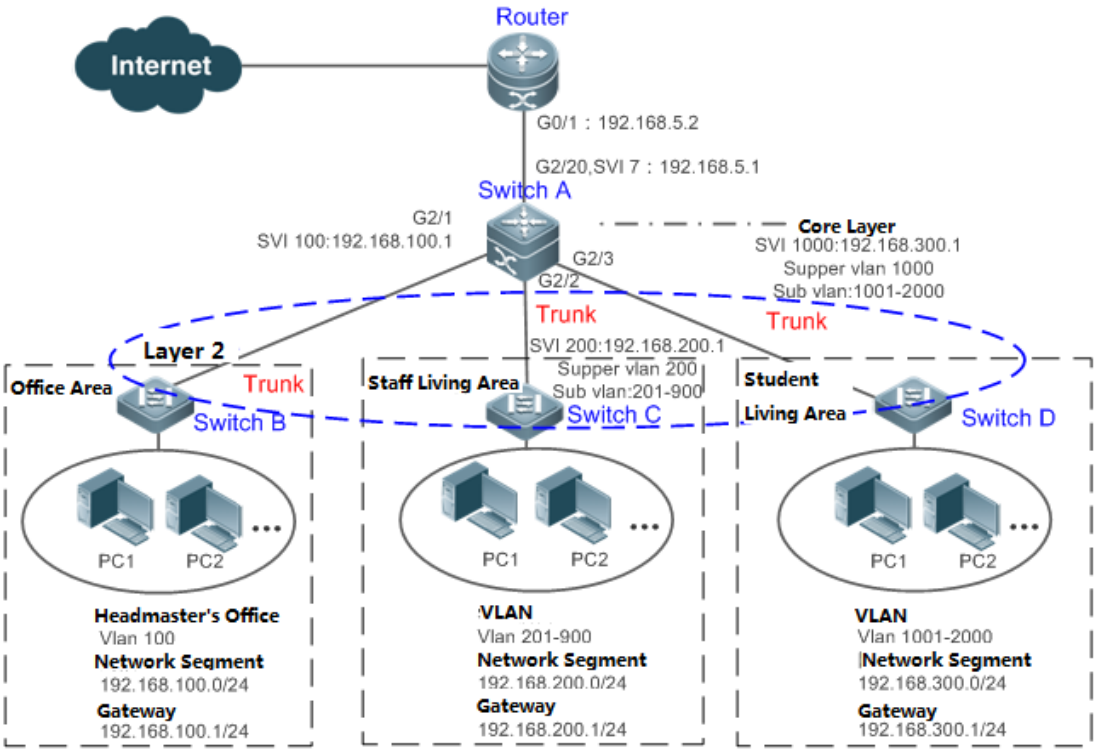


Рисунок 4-2.

Шаги настройки	На коммутаторе A (который является устройством шлюза ядра) установите режим аутентификации на аутентификацию шлюза
Коммутатор A	SwitchA(config)#auth-mode gateway Please save config and reload system. SwitchA(config)#exit *Nov 7 10:13:27: %SYS-5-CONFIG_I: Configured from console by console SwitchA#reload Reload system?(Y/N)y SwitchA#
Проверка	Используйте команду **show running**, чтобы проверить, вступила ли в силу конфигурация
Коммутатор A	SwitchA(config)#show running-config | include auth-mode auth-mode gateway SwitchA(config)#

4.3.2. Настройка VLAN с освобождением от аутентификации

4.3.2.1. Эффект конфигурации

Настройте виртуальные локальные сети с освобождением от аутентификации, чтобы пользователи в этих виртуальных локальных сетях могли получать доступ к Интернету без использования dot1x или веб-аутентификации.

4.3.2.2. Уведомления

Виртуальные локальные сети с освобождением от аутентификации означают только то, что пользователям в этих виртуальных локальных сетях не нужно проходить проверку, связанную с аутентификацией доступа, но все же они должны проходить проверку на основе security ACL. Если указанные пользователи или сети VLAN запрещены в соответствии с security ACL, соответствующие пользователи по-прежнему не могут получить доступ к Интернету. Поэтому во время настройки ACL необходимо убедиться, что указанные VLAN или указанные пользователи в VLAN без аутентификации не заблокированы, если вы надеетесь, что пользователи в VLAN с освобождением от аутентификации смогут получить доступ к Интернету без аутентификации.

4.3.2.3. Шаги настройки

Настройка VLAN с освобождением от аутентификации

- Дополнительная конфигурация. Чтобы избавить всех пользователей в определенных VLAN от dot1x или веб-аутентификации, настройте эти VLAN как VLAN с освобождением от аутентификации.
- Выполните эту настройку на коммутаторах доступа, конвергенции или ядра в зависимости от распределения пользователей.

Команда	**[no] direct-vlan** *vlanlist*
Описание параметров	**no**: если команда содержит этот параметр, это означает, что конфигурация VLAN с освобождением от аутентификации будет удалена. *vlanlist*: этот параметр указывает список сетей VLAN без идентификации, которые необходимо настроить или удалить
По умолчанию	VLAN с освобождением от аутентификации не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы настроить или удалить VLAN с освобождением от аутентификации

4.3.2.4. Проверка

Проверьте конфигурацию VLAN без аутентификации, используя следующий метод:

Включите аутентификацию dot1x на downlink-портах, которые подключаются к пользовательским терминалам, добавьте downlink-порты, которые подключаются к пользовательским терминалам, в определенную виртуальную локальную сеть и настройте

виртуальную локальную сеть как виртуальную локальную сеть без идентификации. Затем откройте Internet Explorer и введите действительный адрес экстрасети (например, www.qtech.ru). Если пользователи могут открыть соответствующую веб-страницу в Интернете, это означает, что VLAN с освобождением от аутентификации действительна; в противном случае VLAN с освобождением от аутентификации не действует.

Используйте команду **show direct-vlan**, чтобы проверить конфигурацию VLAN без аутентификации на устройстве.

Команда	**show direct-vlan**
Командный режим	Привилегированный режим EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Режим глобальной конфигурации
Пример использования	QTECH#show direct-vlan direct-vlan 100

4.3.2.5. Примеры конфигурации

ПРИМЕЧАНИЕ: в следующем примере конфигурации описывается только конфигурация, связанная с SCC.

Настройте VLAN без идентификации, чтобы определенные пользователи могли получить доступ к Интернету без идентификации.

Сценарий:

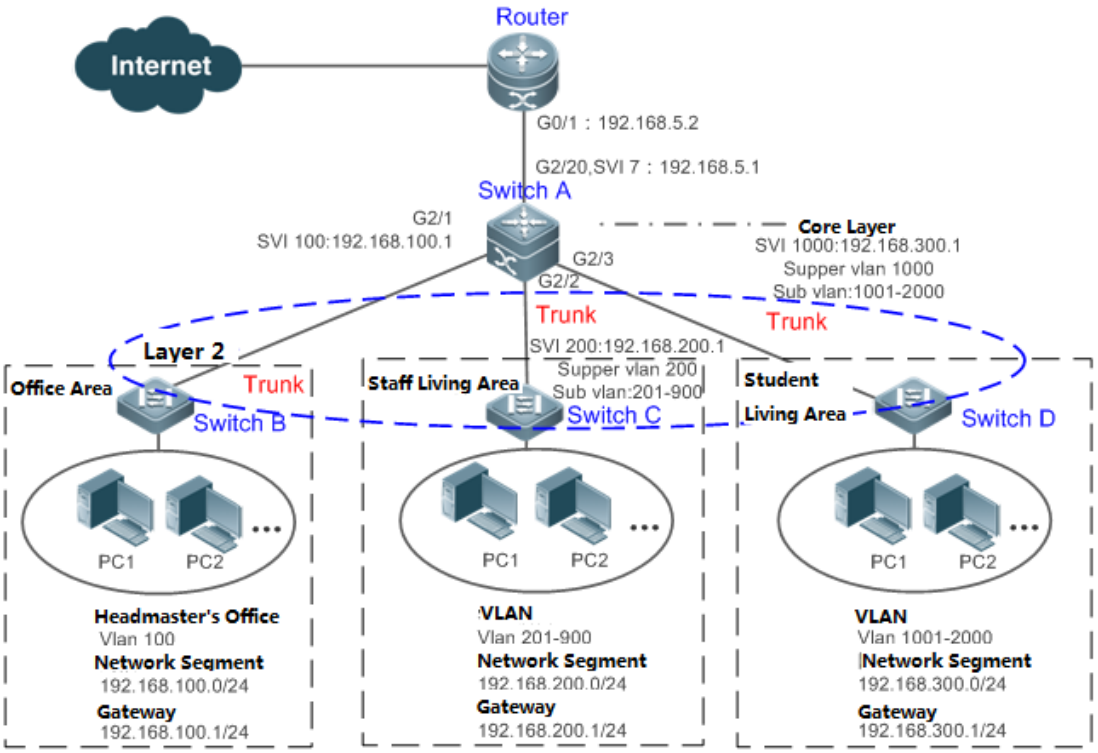


Рисунок 4-3.

Шаги настройки	• На коммутаторе A (который является основным устройством шлюза) установите порт GI 2/1 в качестве магистрального порта и включите аутентификацию dot1x на этом порту. • На коммутаторе A (который является устройством шлюза ядра) настройте VLAN 100, к которой принадлежит офис директора, как VLAN без идентификации
Коммута-тор A	SwitchA(config)#vlan 100 SwitchA(config-vlan)#exit SwitchA(config)#direct-vlan 100 SwitchA(config)#int GigabitEthernet 0/1 SwitchA(config-if-GigabitEthernet 0/1)#switchport mode trunk SwitchA(config-if-GigabitEthernet 0/1)#dot1x port-control auto *Oct 17 16:06:45: %DOT1X-6-ENABLE_DOT1X: Able to receive EAPOL packet and DOT1X authentication enabled
Проверка	• Откройте Internet Explorer с любого ПК в кабинете директора, введите действующий адрес экстрасети и убедитесь, что соответствующую веб-страницу можно открыть. • Используйте команду **show direct-vlan**, чтобы проверить, действительна ли VLAN с освобождением от аутентификации

Коммута-тор A	SwitchA(config)#show direct-vlan direct-vlan 100

4.3.3. Настройка количества пользователей IPv4

4.3.3.1. Эффект конфигурации

Настройте количество пользователей IPv4, чтобы ограничить количество пользователей, которым разрешен доступ к порту доступа.

4.3.3.2. Метод конфигурации

Настройка количества пользователей IPv4

- Дополнительная конфигурация. Чтобы ограничить максимальное количество пользователей, которым разрешен доступ к порту доступа, настройте емкость пользователей IPv4. По умолчанию количество пользователей доступа не ограничено портом доступа. Предположим, ограничение емкости пользователя настроено на конкретном интерфейсе. Когда количество аутентифицированных пользователей на интерфейсе достигает максимума, новые пользователи не могут аутентифицироваться на этом интерфейсе и не могут подключаться к сети до тех пор, пока существующие аутентифицированные пользователи не отключатся от интерфейса.
- Выполните эту настройку на коммутаторах доступа, которые могут быть коммутаторами доступа на границе сети или шлюзами ядра.

Команда	**nac-author-user maximum** *max-user-num* **no nac-author-user maximum**
Описание параметров	**no**: если команда содержит этот параметр, это означает, что ограничение на пропускную способность пользователя доступа IPv4 будет снято с порта. *max-user-num*: этот параметр указывает максимальное количество пользователей IPv4, которым разрешен доступ к порту. Диапазон значений от 1 до 1024
По умолчанию	Количество пользователей доступа IPv4 не ограничено
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду, чтобы ограничить количество пользователей доступа IPv4 к определенному порту доступа

4.3.3.3. Проверка

Проверьте конфигурацию пропускной способности пользователя IPv4 на порту, используя следующий метод:

- Аутентификация dot1x: когда количество пользователей, которые подключаются к сети на основе 1x client-аутентификации на порту, достигает указанной пропускной

способности, ни один новый пользователь не может подключиться к сети через этот порт.

- Веб-аутентификация: когда количество пользователей, которые подключаются к сети на основе веб-аутентификации на порту, достигает указанного количества пользователей, ни один новый пользователь не может подключиться к сети через этот порт.
- Используйте команду **show nac-author-user** [**interface** *interface-name*], чтобы проверить емкость пользователя IPv4, настроенную на устройстве.

Команда	**show nac-author-user** [**interface** *interface-name*]
Описание параметров	*interface-name*: этот параметр указывает имя интерфейса
Командный режим	Привилегированный режим EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Режим глобальной конфигурации
Пример использования	QTECH#show nac-author-user interface GigabitEthernet 0/1 Port Cur_num Max_num -------- ------- ------- Gi0/1 0 4

4.3.3.4. Примеры конфигурации

ПРИМЕЧАНИЕ: в следующем примере конфигурации описывается только конфигурация, связанная с SCC.

Ограничение количества пользователей IP4 на порту для предотвращения влияния терминалов доступа на сеть

Сценарий:

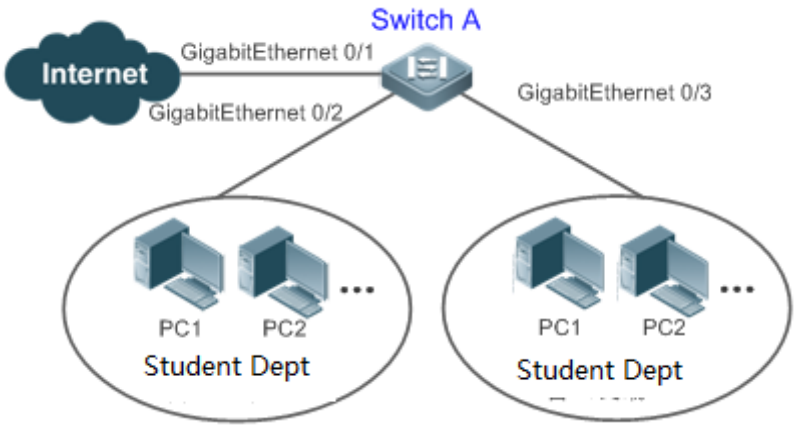


Рисунок 4-4.

Шаги настройки	• Предположим, что среда аутентификации dot1x правильно настроена на коммутаторе доступа A, а аутентификация dot1x включена на порту Gi 0/2. • Установите максимальное количество пользователей доступа IPv4 на порту Gi 0/2 равным 4
Коммутатор A	SwitchA(config)#int GigabitEthernet 0/2 SwitchA(config-if-GigabitEthernet 0/2)#nac-author-user maximum 4
Проверка	• Выполните аутентификацию dot1x для всех четырех компьютеров в общежитии, чтобы компьютеры подключились к сети. Затем возьмите дополнительный терминал для доступа к сети и попытайтесь выполнить аутентификацию dot1x для этого терминала. Убедитесь, что терминал не может быть успешно аутентифицирован для подключения к сети. • Используйте команду **show nac-author-user**, чтобы проверить, вступила ли конфигурация в силу
Коммутатор A	SwitchA(config)#show nac-author-user Port Cur_num Max_num -------- ------- ------- Gi0/1 0 4

4.3.4. Настройка миграции авторизованных пользователей

4.3.4.1. Эффект конфигурации

По умолчанию, когда пользователь подключается к сети после прохождения dot1x или веб-аутентификации в физическом местоположении (которое представлено определенным портом доступа плюс номер VLAN) и быстро перемещается в другое физическое местоположение, не выходя из сети, пользователь не может подключиться к сети через dot1x или веб-аутентификация из нового физического расположения, если функция миграции аутентифицированных пользователей не была настроена заранее.

4.3.4.2. Меры предосторожности

Если функция миграции пользователей, прошедших проверку подлинности, еще не настроена, онлайн-пользователь не сможет подключиться к сети из нового физического местоположения после быстрого перемещения из одного физического местоположения в другое без предварительного выхода в автономный режим. Однако, если пользователь выходит из сети до изменения физического местоположения или отключается во время изменения местоположения, пользователь по-прежнему может нормально подключаться к сети после аутентификации в новом физическом расположении, даже если функция миграции аутентифицированных пользователей не настроена.

4.3.4.3. Метод конфигурации

Настройка миграции авторизованных пользователей

- Дополнительная конфигурация. Чтобы разрешить пользователям проходить аутентификацию и подключаться к сети из разных физических местоположений, включите функцию миграции аутентифицированных пользователей.
- Выполните эту настройку на коммутаторах доступа, конвергенции или ядра в зависимости от распределения пользователей.

Команда	**[no] station-move permit**
Описание параметров	**no station-move permit**: указывает, что миграция пользователей, прошедших аутентификацию, не разрешена. **station-move permit**: указывает, что миграция аутентифицированных пользователей разрешена
По умолчанию	Миграция пользователей, прошедших аутентификацию, не разрешена; то есть, когда пользователь подключается к сети из одного физического местоположения в сети, перемещается в другое физическое местоположение и пытается подключиться к сети из нового физического местоположения, не отключившись сначала от сети, аутентификация завершается неудачей, и пользователь не может подключиться к сети из нового физического местоположения
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для настройки миграции пользователей, прошедших аутентификацию

4.3.4.4. Проверка

- Проверьте конфигурацию миграции аутентифицированных пользователей, используя следующий метод:
- ПК проходит аутентификацию и подключается к сети через порт устройства на основе dot1x с помощью клиента dot1x SU и не отключается активно. Переместите ПК на другой порт устройства, на котором включена аутентификация dot1x, и повторите аутентификацию dot1x. Проверьте, может ли ПК успешно подключиться к сети.

4.3.4.5. Примеры конфигурации

ПРИМЕЧАНИЕ: в следующем примере конфигурации описывается только конфигурация, связанная с SCC.

Настройка миграции онлайн-пользователей, чтобы онлайн-пользователь мог выполнять аутентификацию и подключаться к сети с разных портов без предварительного выхода в автономный режим

Сценарий:

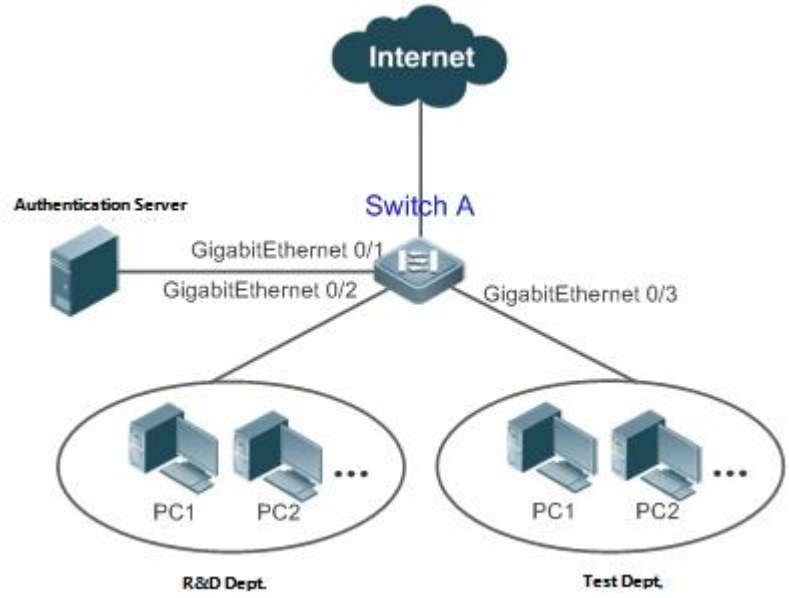


Рисунок 4-5.

Шаги настройки	• Включите аутентификацию dot1x на портах доступа Gi 0/2 и Gi 0/3 и настройте параметры аутентификации. Аутентификация основана на MAC-адресе. • Настройте миграцию онлайн-пользователей
Коммута-тор A	sw1(config)#station-move permit
Проверка	Ноутбук в отделе исследований и разработок выполняет аутентификацию с помощью клиента dot1x SU и подключается к сети. Отсоедините сетевой кабель от ПК, подключите ПК к локальной сети, в которой находится отдел тестирования, и снова выполните аутентификацию dot1x для ПК с помощью клиента dot1x SU. Убедитесь, что компьютер может успешно подключиться к сети
Коммута-тор A	sw1(config)#show running-config | include station station-move permit

4.3.5. Настройка определения онлайн-статуса пользователя

4.3.5.1. Эффект конфигурации

После включения функции определения онлайн-статуса пользователя, если трафик пользователя ниже определенного порога в течение заданного периода времени,

устройство автоматически отключает пользователя, чтобы избежать экономических потерь, связанных с постоянным взиманием платы с пользователя.

4.3.5.2. Меры предосторожности

Следует отметить, что, если настроено отключение пользователей с нулевым трафиком, обычно программное обеспечение, такое как 360 Security Guard, будет работать на пользовательском терминале по умолчанию. Тогда такое ПО будет посылать пакеты снова и снова, и устройство отключит пользователя только тогда, когда его терминал выключен.

4.3.5.3. Метод конфигурации

Настройка определения онлайн-статуса пользователя

- Дополнительная конфигурация. Пользователь отключается, если пользователь не использует трафик в течение восьми часов по умолчанию.
- Выполните эту настройку на коммутаторах доступа, конвергенции или ядра в зависимости от распределения пользователей. Конфигурация действует только на сконфигурированное устройство, а не на другие устройства в сети.
- Если для параметра порога трафика установлено значение 0, это означает, что будет выполняться обнаружение нулевого трафика.

Команда	**offline-detect interval** *interval* **threshold** *threshold* **no offline-detect** **default offline-detect**
Описание параметров	*interval*: этот параметр указывает интервал обнаружения в автономном режиме. Диапазон значений составляет от 6 до 65 535 минут на коммутаторе или от 1 до 65 535 минут на устройстве без коммутатора. Значение по умолчанию — 8 часов, то есть 480 минут. *threshold*: этот параметр указывает пороговое значение трафика. Диапазон значений от 0 до 4 294 967 294 в байтах. Значение по умолчанию равно 0, что указывает на то, что пользователь отключается, когда трафик пользователя не обнаружен. **no offline-detect**: отключает функцию определения онлайн-статуса пользователя. **default offline-detect**: восстанавливает значение по умолчанию. Другими словами, онлайн-пользователь будет отключен, когда устройство обнаружит, что у пользователя нет трафика в течение восьми часов
По умолчанию	8 часов
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы настроить определение онлайн-статуса пользователя, чтобы пользователь отключался, когда его трафик ниже определенного порога в течение определенного периода времени. Используйте команду **no offline-detect**, чтобы отключить функцию обнаружения пользовательского онлайн-статуса,

	или используйте команду **default offline-detect**, чтобы восстановить режим обнаружения по умолчанию

4.3.5.4. Проверка

Проверьте конфигурацию определения онлайн-статуса пользователя, используя следующий метод:

- После включения функции определения онлайн-статуса пользователя выключите указанный аутентифицированный терминал после того, как соответствующий пользователь подключится к сети. Затем подождите указанный период времени и запустите на устройстве команду запроса онлайн-пользователя, связанную с dot1x или веб-аутентификацией, чтобы убедиться, что пользователь уже находится в автономном режиме.

4.3.5.5. Примеры конфигурации

ПРИМЕЧАНИЕ: в следующем примере конфигурации описывается только конфигурация, связанная с SCC.

Настройка определения онлайн-статуса пользователя таким образом, чтобы пользователь отключался, если у пользователя нет трафика в течение пяти минут

Сценарий:

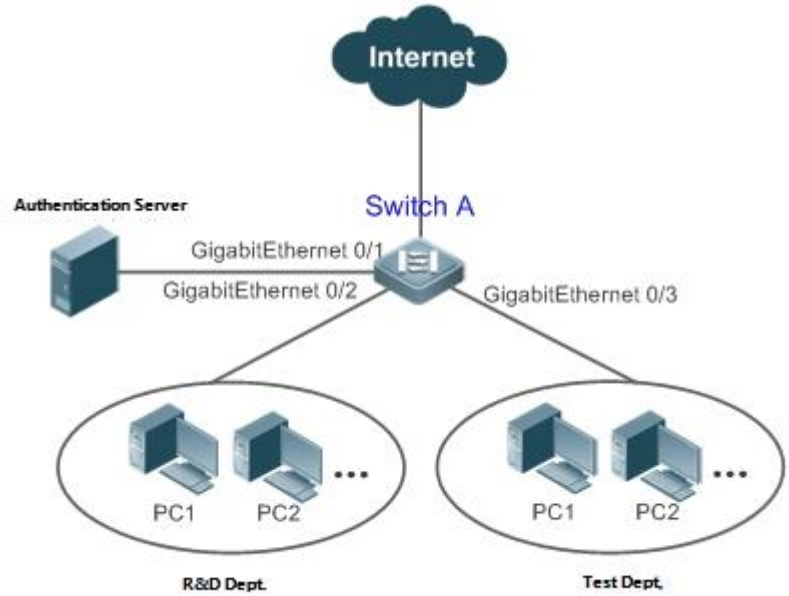


Рисунок 4-6.

Шаги настройки	• Включите аутентификацию dot1x на порту доступа Gi 0/2 и настройте параметры аутентификации. Аутентификация основана на MAC-адресе. • Настройте определение онлайн-статуса пользователя, чтобы пользователь отключался, если у него нет трафика в течение пяти минут

Коммутатор A	sw1(config)# offline-detect interval 5 threshold 0
Проверка	Выполните аутентификацию dot1x с помощью клиента dot1x SU для ПК в отделе исследований и разработок, чтобы ПК подключился к сети. Затем выключите компьютер, подождите 6 минут и запустите команду онлайн-пользователя, доступную с аутентификацией dot1x, на коммутаторе 1, чтобы убедиться, что пользователь ПК уже находится в автономном режиме
Коммутатор A	sw1(config)#show running-config | include offline-detect offline-detect interval 5

4.4. Мониторинг

4.4.1. Отображение

Команда	Функция
show direct-vlan	Отображает конфигурацию VLAN без аутентификации
show nac-author-user [**interface** *interface-name*]	Отображает информацию о пользовательских записях IPv4 на определенном интерфейсе

4.4.2. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому закройте переключатель отладки сразу после использования.

Команда	Функция
debug scc event	Отладка работающего процесса SCC
debug scc user [**mac** | **author** | **mac**]	Отладка пользовательских записей SCC
debug scc acl-show summary	Отладка списков управления доступом, хранящихся в текущем SCC и доставляемых различными службами
debug scc acl-show all	Отладка всех ALC, хранящихся в текущем SCC

5. НАСТРОЙКА ПОЛИТИКИ ПАРОЛЕЙ

5.1. Обзор

Политика паролей — это функция защиты паролем, предназначенная для локальной аутентификации устройства. Он настроен для контроля паролей пользователей и состояний входа в систему.

ПРИМЕЧАНИЕ: в следующих разделах представлена только политика паролей.

5.2. Функции

5.2.1. Базовые концепты

Минимальная длина пароля

Администраторы могут установить минимальную длину паролей пользователей в соответствии с требованиями безопасности системы. Если пароль, введенный пользователем, короче минимальной длины пароля, система не позволяет пользователю установить этот пароль, а отображает подсказку, предлагая пользователю указать другой пароль соответствующей длины.

Обнаружение надежного пароля

Чем проще пароль, тем выше вероятность его взлома. Например, пароль, который совпадает с паролем соответствующей учетной записи, или простой пароль, содержащий только символы или цифры, может быть легко взломан. В целях безопасности администраторы могут включить функцию обнаружения надежных паролей, чтобы пароли, устанавливаемые пользователями, были очень сложными. После включения функции определения надежного пароля будет отображаться запрос для следующих типов паролей:

1. Пароли, которые совпадают с соответствующими учетными записями.
2. Простые пароли, содержащие только символы или цифры.

Жизненный цикл пароля

Жизненный цикл пароля определяет время действия пароля пользователя. Когда время обслуживания пароля превышает жизненный цикл, пользователю необходимо сменить пароль.

Если пользователь вводит пароль, срок действия которого уже истек во время входа в систему, система выдаст подсказку, указывающую, что срок действия пароля истек, и пользователю необходимо сбросить пароль. Если новый пароль, введенный во время сброса пароля, не соответствует системным требованиям или новые пароли, введенные дважды подряд, не совпадают, система попросит пользователя ввести новый пароль еще раз.

Защита от повторного использования паролей

При смене пароля пользователь установит новый пароль, а старый пароль будет записан как запись истории пользователя. Если новый пароль, введенный пользователем, уже использовался ранее, система выдает сообщение об ошибке и просит пользователя указать другой пароль.

Можно настроить максимальное количество записей истории паролей на пользователя. Когда количество записей истории паролей пользователя превышает максимальное количество, настроенное для этого пользователя, новая запись истории паролей перезапишет самую старую запись истории паролей пользователя.

Хранение зашифрованных паролей

Администраторы могут включить хранение зашифрованных паролей из соображений безопасности. Когда администраторы запускают команду **show running-config** для отображения конфигурации или запускают команду **write** для сохранения файлов конфигурации, различные пароли, установленные пользователем, отображаются в формате зашифрованного текста. Если администраторы отключат хранение зашифрованных паролей в следующий раз, пароли, уже имеющиеся в зашифрованном текстовом формате, не будут восстановлены в пароли в виде открытого текста.

5.3. Конфигурация

Конфигурация	Описание и команда	
Настройка политики безопасности паролей	Необязательная конфигурация, которая используется для настройки комбинации параметров, связанных с политикой безопасности паролей	
	password policy life-cycle	Настраивает жизненный цикл пароля
	password policy min-size	Настраивает минимальную длину паролей пользователей
	password policy no-repeat-times	Устанавливает время без повторения последней конфигурации пароля, чтобы пароли, указанные в это время последней конфигурации пароля, больше нельзя было использовать в будущей конфигурации пароля
	password policy strong	Включает функцию обнаружения надежного пароля
	service password-encryption	Устанавливает хранилище зашифрованных паролей

5.3.1. Настройка политики безопасности паролей

5.3.1.1. Сетевые требования

Предоставьте политику безопасности паролей для локальной аутентификации устройства. Пользователи могут настраивать различные политики безопасности паролей для реализации управления безопасностью паролей.

5.3.1.2. Примечания

Настроенная политика безопасности паролей действительна для глобальных паролей (настраиваемых с помощью команд **enable password** и **enable secret**) и паролей

локальных пользователей (настраиваемых с помощью команды **username** *name* **password** *password*). Он недействителен для паролей в режиме line.

5.3.1.3. Шаги настройки

Настройка жизненного цикла пароля

- Опционально
- Выполните эту настройку на каждом устройстве, для которого требуется настройка жизненного цикла пароля, если не указано иное.

Настройка минимальной длины паролей пользователей

- Опционально
- Выполните эту настройку на каждом устройстве, для которого требуется ограничение на минимальную длину паролей пользователей, если не указано иное.

Установка времени запрета повторения последней конфигурации пароля

- Опционально
- Выполните эту настройку на каждом устройстве, для которого требуется ограничение времени неповторения последней конфигурации пароля, если не указано иное.

Включение функции определения надежного пароля

- Опционально
- Выполните эту настройку на каждом устройстве, для которого требуется определение надежного пароля, если не указано иное.

Настройка хранилища зашифрованных паролей

- Опционально
- Выполните эту настройку на каждом устройстве, для которого требуется хранение паролей в зашифрованном формате, если не указано иное.

5.3.1.4. Проверка

Настройте локального пользователя на устройстве и настройте действительный пароль и недопустимый пароль для пользователя.

- При настройке действительного пароля устройство правильно добавляет пароль.
- При настройке неверного пароля устройство отображает соответствующий журнал ошибок.

5.3.1.5. Связанные команды

Настройка жизненного цикла пароля

Команда	**password policy life-cycle** *days*
Описание параметров	**life-cycle** *days*: указывает жизненный цикл пароля в днях. Диапазон значений от 1 до 65 535
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Жизненный цикл пароля используется для определения срока действия паролей пользователей. Если пользователь входит в систему с паролем, время обслуживания которого уже превышает жизненный цикл, выдается подсказка, предлагающая пользователю изменить пароль

Настройка минимальной длины паролей пользователей

Команда	**password policy min-size** *length*
Описание параметров	**min-size** *length*: указывает минимальную длину паролей. Диапазон значений от 1 до 31
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки минимальной длины паролей. Если минимальная длина паролей не настроена, пользователи могут вводить пароль любой длины

Установка времени запрета повторения последней конфигурации пароля

Команда	**password policy no-repeat-times** *times*
Описание параметров	**no-repeat-times** *times*: указывает время без повторения последней конфигурации пароля. Диапазон значений от 1 до 31
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения этой функции все старые пароли, использованные несколько раз при последней настройке пароля, будут записаны как записи истории паролей пользователя. Если новый пароль, введенный пользователем, уже использовался ранее, система выдает сообщение об ошибке, и изменение пароля завершается неудачно. Вы можете настроить максимальное количество записей истории паролей для каждого пользователя. Когда количество записей истории паролей пользователя превышает максимальное количество, настроенное для пользователя, новая запись истории паролей перезапишет самую старую запись истории паролей пользователя

Включение функции определения надежного пароля

Команда	**password policy strong**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения функции определения надежного пароля отображается запрос для следующих типов паролей: 1. Пароли, которые совпадают с соответствующими учетными записями. 2. Простые пароли, содержащие только символы или цифры

Настройка хранилища зашифрованных паролей

Команда	**service password-encryption**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	До того, как будет настроено хранение зашифрованных паролей, все пароли, используемые в процессе настройки, будут отображаться и сохраняться в формате открытого текста, если только пароли не настроены в формате зашифрованного текста. Вы можете включить хранение зашифрованных паролей из соображений безопасности. Когда вы запускаете команду **show running-config** для отображения конфигурации или запускаете команду **write** для сохранения файлов конфигурации, различные пароли, установленные пользователем, отображаются в формате зашифрованного текста. Если вы отключите хранение зашифрованных паролей в следующий раз, пароли, уже находящиеся в зашифрованном текстовом формате, не будут восстановлены в пароли в виде открытого текста

Проверка информации о политике безопасности с настроенным пользователем паролем

Команда	**show password policy**
Командный режим	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду для отображения политики безопасности паролей, настроенной на устройстве

5.3.1.6. Примеры конфигурации

ПРИМЕЧАНИЕ: в следующем примере конфигурации описывается конфигурация, связанная с политикой безопасности паролей.

Настройка проверки безопасности пароля на устройстве

Типичное применение	Предположим, что в сетевой среде возникают следующие требования к безопасности пароля: 1. Минимальная длина паролей — 8 символов. 2. Жизненный цикл пароля составляет 90 дней. 3. Пароли хранятся и передаются в зашифрованном текстовом формате. 4. Количество неповторяющихся записей истории паролей равно 3. 5. Пароли не должны совпадать с именами пользователей и не должны содержать только простые символы или цифры
Шаги настройки	• Установите минимальную длину паролей на 8. • Установите жизненный цикл пароля на 90 дней. • Включить хранение зашифрованных паролей. • Установите количество повторов записей истории паролей на 3. • Включите функцию определения надежного пароля
	QTECH# configure terminal QTECH(config)# password policy min-size 8 QTECH(config)# password policy life-cycle 90 QTECH(config)# service password-encryption QTECH(config)# password policy no-repeat-times 3 QTECH(config)# password policy strong
Проверка	Когда вы создаете пользователя и соответствующий пароль после настройки политики безопасности паролей, система выполнит соответствующее обнаружение в соответствии с политикой безопасности паролей. Запустите команду **show password policy**, чтобы отобразить информацию о настроенной пользователем политике безопасности паролей
	QTECH# show password policy Global password policy configurations: Password encryption: Enabled Password strong-check: Enabled Password min-size: Enabled (8 characters) Password life-cycle: Enabled (90 days) Password no-repeat-times: Enabled (max history record: 3)

5.3.1.7. Распространенные ошибки

Время, настроенное для предоставления пользователю предварительного предупреждения об истечении срока действия пароля, превышает жизненный цикл пароля.

5.4. Мониторинг

5.4.1. Отображение

Команда	Функция
show password policy	Отображает информацию о политике безопасности паролей, настроенной пользователем

6. НАСТРОЙКА STORM CONTROL

6.1. Обзор

Когда локальная сеть (LAN) имеет избыточные потоки широковещательных данных, потоки многоадресных данных или неизвестные потоки одноадресных данных, скорость сети будет снижаться, а передача пакетов будет иметь повышенную вероятность тайм-аута. Эта ситуация называется LAN storm. Storm может возникнуть при неправильном выполнении протокола топологии или конфигурации сети.

Storm Control может быть реализован для ограничения потоков широковещательных данных, многоадресных потоков данных или неизвестных одноадресных потоков данных. Если скорость потоков данных, полученных портом устройства, находится в пределах настроенного порога пропускной способности, порога количества пакетов в секунду или порога в килобитах в секунду, потокам данных разрешается проходить. Если скорость превышает пороговые значения, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах пороговых значений. Это предотвращает флуд данных в локальную сеть, вызывая storm.

6.2. Приложения

Приложение	Описание
Предотвращение сетевых атак	Включает Storm Control для предотвращения флудинга

6.2.1. Предотвращение сетевых атак

6.2.1.1. Сценарий

Требования к приложениям для предотвращения сетевых атак описываются следующим образом:

- Защитите устройства от флудинга широковещательных пакетов, многоадресных пакетов или неизвестных одноадресных пакетов.

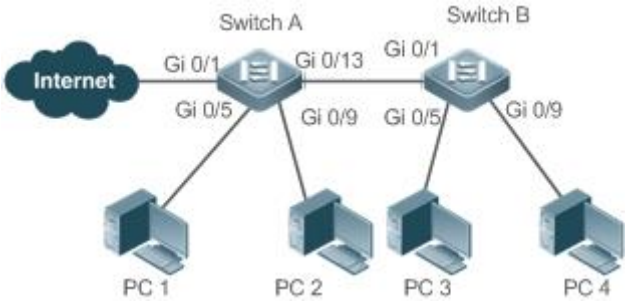


Рисунок 6-1.

Коммутатор A и коммутатор B являются устройствами доступа.

ПК 1, ПК 2, ПК 3 и ПК 4 — это настольные компьютеры.

6.2.1.2. Развертывание

Включите Storm Control на портах всех устройств доступа (коммутатор A и коммутатор B).

6.3. Функции

6.3.1. Базовые концепты

Storm Control

Если скорость потоков данных (широковещательных пакетов, многоадресных пакетов или неизвестных одноадресных пакетов), полученных портом устройства, находится в пределах настроенного порога пропускной способности, порога количества пакетов в секунду или порога в килобитах в секунду, потоки данных пропускаются. Если скорость превышает пороговые значения, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах пороговых значений.

Storm Control на основе порога пропускной способности

Если скорость потоков данных, полученных портом устройства, находится в пределах настроенного порога пропускной способности, потоки данных могут проходить. Если скорость превышает пороговое значение, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах порогового значения.

Storm Control на основе порога количества пакетов в секунду

Если скорость потоков данных, полученных портом устройства, находится в пределах настроенного порога пакетов в секунду, потоки данных могут пройти. Если скорость превышает пороговое значение, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах порогового значения.

Storm Control на основе порогового значения килобит в секунду

Если скорость потоков данных, полученных портом устройства, находится в пределах настроенного порогового значения в килобитах в секунду, потоки данных могут пройти. Если скорость превышает пороговое значение, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах порогового значения.

6.3.2. Обзор

Особенность	Описание
Storm Control одноадресных пакетов	Ограничивает неизвестные одноадресные пакеты для предотвращения флудинга
Storm Control многоадресных пакетов	Ограничивает многоадресные пакеты для предотвращения флудинга
Storm Control широковещательных пакетов	Ограничивает широковещательные пакеты для предотвращения флудинга

6.3.3. Storm Control одноадресных пакетов

Функция Storm Control одноадресных пакетов отслеживает скорость неизвестных одноадресных потоков данных, полученных портом устройства, чтобы ограничить трафик локальной сети и предотвратить флудинг, вызванный избыточными потоками данных.

6.3.3.1. Принцип работы

Если скорость неизвестных одноадресных потоков данных, полученных портом устройства, находится в пределах настроенного порога пропускной способности, порога количества пакетов в секунду или порога в килобитах в секунду, потокам данных разрешено проходить. Если скорость превышает пороговые значения, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах пороговых значений.

6.3.3.2. Связанная конфигурация

Включение Storm Control одноадресных пакетов на портах

По умолчанию Storm Control одноадресных пакетов на портах отключено.

Запустите команду **storm-control unicast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }] для включения Storm Control одноадресных пакетов на портах.

Запустите команду **no storm-control unicast** или **default storm-control unicast**, чтобы отключить Storm Control одноадресных пакетов на портах.

Параметры команды по умолчанию определяются сопутствующими продуктами.

6.3.4. Storm Control многоадресных пакетов

Функция Storm Control многоадресных пакетов отслеживает скорость потоков многоадресных данных, полученных портом устройства, чтобы ограничить трафик локальной сети и предотвратить флудинг, вызванный избыточными потоками данных.

6.3.4.1. Принцип работы

Если скорость многоадресных потоков данных, полученных портом устройства, находится в пределах настроенного порога пропускной способности, порога количества пакетов в секунду или порога в килобитах в секунду, потокам данных разрешено проходить. Если скорость превышает пороговые значения, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах пороговых значений.

6.3.4.2. Связанная конфигурация

Включение Storm Control многоадресных пакетов на портах

По умолчанию Storm Control многоадресных пакетов на портах отключено.

Запустите команду **storm-control multicast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }] для включения Storm Control многоадресных пакетов на портах.

Запустите команду **no storm-control multicast** или **default storm-control multicast**, чтобы отключить Storm Control многоадресных пакетов на портах.

Параметры команды по умолчанию определяются сопутствующими продуктами.

6.3.5. Storm Control широковещательных пакетов

Функция Storm Control широковещательных пакетов отслеживает скорость потоков широковещательных данных, полученных портом устройства, чтобы ограничить трафик локальной сети и предотвратить флудинг, вызванный избыточными потоками данных.

6.3.5.1. Принцип работы

Если скорость широковещательных потоков данных, полученных портом устройства, находится в пределах настроенного порога пропускной способности, порога количества пакетов в секунду или порога в килобитах в секунду, потокам данных разрешено

проходить. Если скорость превышает пороговые значения, избыточные потоки данных отбрасываются до тех пор, пока скорость не упадет в пределах пороговых значений.

6.3.5.2. Связанная конфигурация

Включение Storm Control широковещательных пакетов на портах

По умолчанию Storm Control широковещательных пакетов на портах отключено.

Запустите команду **storm-control broadcast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }] для включения Storm Control широковещательных пакетов на портах.

Запустите команду **no storm-control broadcast** или **default storm-control broadcast**, чтобы отключить Storm Control широковещательных пакетов на портах.

Параметры команды по умолчанию определяются сопутствующими продуктами.

6.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций Storm Control	(Обязательно) Используется для включения Storm Control	
	storm-control { **broadcast** | **multicast** | **unicast**} [{ **level** *percent* | **pps** *packets* | *rate-bps*}]	Включает Storm Control

6.4.1. Настройка основных функций Storm Control

6.4.1.1. Эффект конфигурации

Предотвратите флудинг, вызванный избыточными широковещательными пакетами, многоадресными пакетами и неизвестными одноадресными пакетами.

6.4.1.2. Примечания

Когда вы запускаете команду (например, **storm-control unicast**) для включения Storm Control, если вы не задаете параметры, используются значения по умолчанию.

6.4.1.3. Шаги настройки

Включение Storm Control одноадресных пакетов

- Обязательный.
- Включите Storm Control одноадресных пакетов на каждом устройстве, если не указано иное.

Включение Storm Control многоадресных пакетов

- Обязательный.
- Включите Storm Control многоадресных пакетов на каждом устройстве, если не указано иное.

Включение Storm Control широковещательных пакетов

- Обязательный.
- Включите Storm Control широковещательных пакетов на каждом устройстве, если не указано иное.

6.4.1.4. Проверка

Запустите команду **show storm-control**, чтобы проверить, выполнена ли конфигурация успешно.

6.4.1.5. Связанные команды

Включение Storm Control одноадресных пакетов

Команда	**storm-control unicast** [{ **level** *percent* | **pps** *packets* | *rate-bps*}]
Описание параметров	**level** *percent*: указывает процент порога пропускной способности. **pps** *packets*: указывает количество пакетов в секунду. *rate-bps*: указывает скорость передачи пакетов
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Storm Control может быть включен только на портах коммутатора

Включение Storm Control многоадресных пакетов

Команда	**storm-control multicast** [{ **level** *percent* | **pps** *packets* | *rate-bps*}]
Описание параметров	**level** *percent*: указывает процент порога пропускной способности. **pps** *packets*: указывает количество пакетов в секунду. *rate-bps*: указывает скорость передачи пакетов
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Storm Control может быть включен только на портах коммутатора

Включение Storm Control широковещательных пакетов

Команда	**storm-control broadcast** [{ **level** *percent* | **pps** *packets* | *rate-bps*}]
Описание параметров	**level** *percent*: указывает процент порога пропускной способности. **pps** *packets*: указывает количество пакетов в секунду. *rate-bps*: указывает скорость передачи пакетов
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Storm Control может быть включен только на портах коммутатора

6.4.1.6. Пример конфигурации

Включение Storm Control на устройствах

Сценарий:

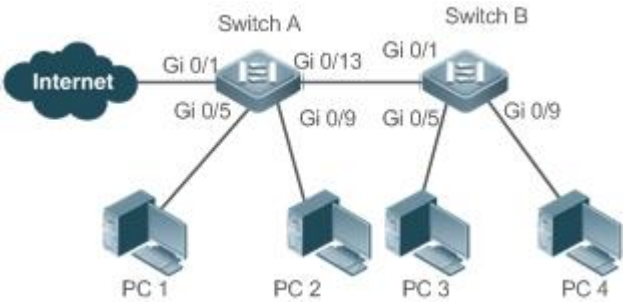


Рисунок 6-2.

Шаг конфигурации	Включите Storm Control на коммутаторе A и коммутаторе B
Коммутатор A	QTECH(config)#interface range gigabitEthernet 0/5,0/9,0/13 QTECH(config-if-range)#storm-control broadcast QTECH(config-if-range)#storm-control multicast QTECH(config-if-range)#storm-control unicast
Коммутатор B	QTECH(config)#interface range gigabitEthernet 0/1,0/5,0/9 QTECH(config-if-range)#storm-control broadcast QTECH(config-if-range)#storm-control multicast QTECH(config-if-range)#storm-control unicast
Проверка	Проверьте, включен ли штормовой контроль на коммутаторе A и коммутаторе B
Коммутатор A	QTECH# sho storm-control Interfac Broadcast Control Multicast Control Unicast Control Action ---------- ---------- ---------- ---------- ---------- GigabitEthernet 0/1 Disabled Disabled Disabled none GigabitEthernet 0/5 default default default none GigabitEthernet 0/9 default default default none GigabitEthernet 0/13 default default default none
Коммутатор B	QTECH#sho storm-control Interface Broadcast Control Multicast Control Unicast Control Action ---------- ---------- ---------- ---------- ---------- GigabitEthernet 0/1 default default default none

	GigabitEthernet 0/5	default	default	default	none
	GigabitEthernet 0/9	default	default	default	none

6.5. Мониторинг

6.5.1. Отображение

Описание	Команда
Отображает информацию о Storm Control	**show storm-control** [*interface-type interface-number*]

7. НАСТРОЙКА SSH

7.1. Обзор

Соединение Secure Shell (SSH) похоже на соединение Telnet, за исключением того, что все данные, передаваемые по SSH, шифруются. Когда пользователь в небезопасной сетевой среде подключается к устройству удаленно, SSH помогает обеспечить информационную безопасность и мощную аутентификацию, защищая устройство от таких атак, как подмена IP-адреса и перехват открытого пароля.

Устройство с поддержкой SSH может быть подключено к нескольким клиентам SSH. Кроме того, устройство также может работать как SSH-клиент и позволяет пользователям устанавливать SSH-соединение с устройством SSH-сервера. Таким образом, локальное устройство может безопасно подключиться к удаленному устройству через SSH для осуществления управления.

ПРИМЕЧАНИЕ: в настоящее время устройство может работать либо как SSH-сервер, либо как SSH-клиент, поддерживая версии SSHv1 и SSHv2. Сервис QTECH SSH поддерживает как IPv4, так и IPv6.

ПРИМЕЧАНИЕ: если не указано иное, SSH в этом документе относится к SSHv2.

7.1.1. Протоколы и стандарты

- RFC 4251: архитектура протокола Secure Shell (SSH).
- RFC 4252: протокол аутентификации Secure Shell (SSH).
- RFC 4253: протокол транспортного уровня Secure Shell (SSH).
- RFC 4254: протокол подключения Secure Shell (SSH).
- RFC 4419: групповой обмен Диффи-Хеллмана для протокола транспортного уровня Secure Shell (SSH).
- RFC 4716: формат файла открытого ключа Secure Shell (SSH).
- RFC 4819: подсистема открытых ключей Secure Shell.
- RFC 3526: более модульные экспоненциальные (MODP) группы Диффи-Хеллмана для обмена ключами через Интернет (IKE).
- RFC 2409: интернет-обмен ключами (IKE).
- RFC 1950: спецификация формата сжатых данных ZLIB, версия 3.3.
- draft-ietf-secsh-filexfer-05: протокол передачи файлов SSH.
- draft-ylonen-ssh-protocol-00: версия протокола удаленного входа SSH — 1.5. Comware реализует функции сервера SSH, но не функции клиента SSH.

7.2. Приложения

Приложение	Описание
Управление SSH-устройствами	Используйте SSH для управления устройствами
Аутентификация по локальной учетной записи SSH	Используйте аутентификацию по паролю локальной учетной записи для аутентификации пользователя SSH

Приложение	Описание
Аутентификация SSH AAA	Используйте режим аутентификации, авторизации и учета (AAA) для аутентификации пользователя SSH
Аутентификация с открытым ключом SSH	Используйте аутентификацию с открытым ключом для аутентификации пользователя SSH
Передача файлов SSH	Используйте команды безопасного копирования (SCP) на клиенте для обмена данными с сервером SSH
SSH-клиентское приложение	Используйте клиент SSH для безопасного входа на удаленное устройство для управления

7.2.1. Управление SSH-устройствами

7.2.1.1. Сценарий

Вы можете использовать SSH для управления устройствами при условии, что функция сервера SSH включена. По умолчанию эта функция отключена. Компонент Telnet, поставляемый с системой Windows, не поддерживает SSH. Поэтому необходимо использовать стороннее клиентское программное обеспечение. В настоящее время хорошо совместимое программное обеспечение включает PuTTY, Linux и SecureCRT. Далее в качестве примера используется PuTTY, чтобы представить конфигурации клиента SSH. Рисунок 7-1 показывает топологию сети.



Рисунок 7-1. Сетевая топология управления устройствами SSH

7.2.1.2. Развертывание

Настройте клиент SSH следующим образом:

- Запустите программу PuTTY.
- На вкладке **Session** сеанса PuTTY введите IP-адрес узла SSH-сервера и номер порта SSH **22** и выберите тип подключения **SSH**.
- На вкладке параметров **SSH** в PuTTY выберите предпочтительную версию протокола SSH **2**.
- На вкладке **SSH authentication** в PuTTY выберите метод аутентификации **Attempt "keyboard-interactive" auth**.
- Нажмите **Open**, чтобы подключиться к SSH-серверу.
- Введите правильное имя пользователя и пароль, чтобы войти в интерфейс входа в терминал.

7.2.2. Аутентификация по локальной учетной записи SSH

7.2.2.1. Сценарий

Клиенты SSH могут использовать режим аутентификации по паролю локальной учетной записи, как показано на Рисунке 7-2. Для обеспечения безопасности обмена данными ПК 1 и ПК 2 работают как клиенты SSH и используют протокол SSH для входа на сетевое устройство, на котором включена функция сервера SSH. Требования следующие:

- Пользователи SSH используют режим аутентификации по паролю локальной учетной записи.
- Пять строк, включая строки 0 и 4, активируются одновременно. Пароль для входа «passzero» для строки 0 и «pass» для остальных линий. Можно использовать любое имя пользователя.

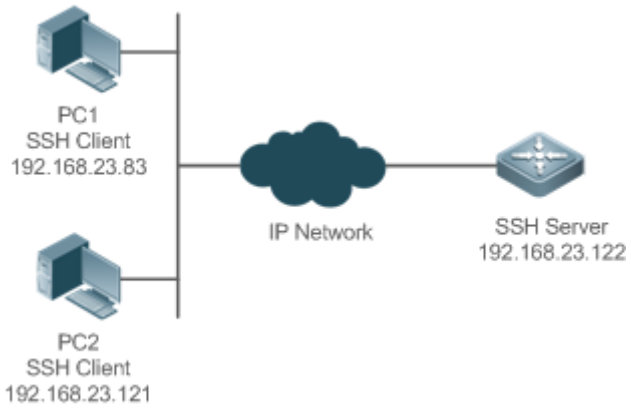


Рисунок 7-2. Сетевая топология аутентификации по паролю локальной строки SSH

7.2.2.2. Развертывание

- Настройте SSH-сервер следующим образом:

1. Включите функцию сервера SSH глобально. По умолчанию сервер SSH поддерживает две версии SSH: SSHv1 и SSHv2.
2. Настройте ключ. С помощью этого ключа сервер SSH расшифровывает зашифрованный пароль, полученный от клиентов SSH, сравнивает расшифрованный открытый текст с паролем, хранящимся на сервере, и возвращает сообщение об успешной или неудачной аутентификации. SSHv1 использует ключ RSA, тогда как SSHv2 использует ключ RSA или DSA.
3. Настройте IP-адрес интерфейса FastEthernet 0/1 на сервере SSH. Клиент SSH подключается к серверу SSH, используя этот IP-адрес. Маршруты от клиентов SSH к серверу SSH доступны.

- Настройте клиент SSH следующим образом:

Доступно разнообразное клиентское программное обеспечение SSH, включая PuTTY, Linux и OpenSSH. В этом документе PuTTY используется в качестве примера для объяснения метода настройки клиентов SSH.

1. Откройте вкладку подключения к PuTTY и выберите SSHv1 для входа в систему с аутентификацией. (Метод аналогичен, если выбран SSHv2.)
2. Укажите IP-адрес и идентификатор подключенного порта SSH-сервера. Как показано в топологии сети, IP-адрес сервера — 192.168.23.122, а идентификатор порта — 22. Нажмите **Open**, чтобы установить соединение. Поскольку текущий режим аутентификации не требует имени пользователя, вы можете ввести

любое имя пользователя, но оно не может быть нулевым. (В этом примере имя пользователя — «anyname».)

7.2.3. Аутентификация SSH AAA

7.2.3.1. Сценарий

Пользователи SSH могут использовать режим аутентификации AAA для аутентификации пользователя, как показано на Рисунке 7-3. Для обеспечения безопасности обмена данными ПК работают как клиенты SSH и используют протокол SSH для входа на сетевое устройство, на котором включен сервер SSH. Чтобы лучше управлять безопасностью, для входа пользователя в систему SSH-клиентов используется режим аутентификации AAA. Два метода аутентификации, включая аутентификацию сервера Radius и локальную аутентификацию, предусмотрены в списке методов аутентификации AAA для обеспечения надежности. Предпочтительным является метод аутентификации сервера Radius. Если сервер Radius не отвечает, он обращается к локальной аутентификации.

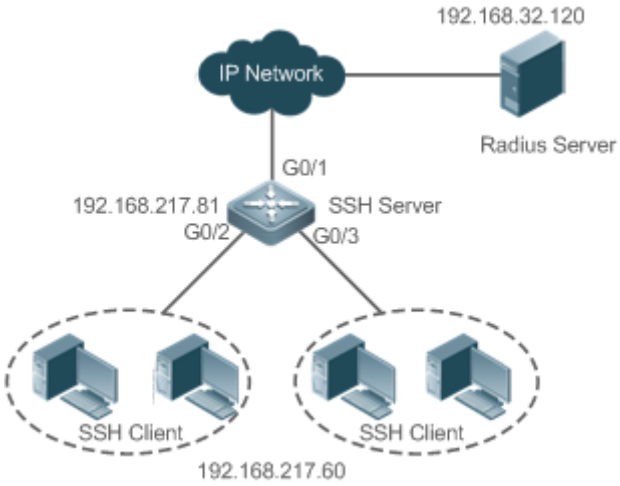


Рисунок 7-3. Сетевая топология аутентификации SSH AAA

7.2.3.2. Развертывание

- Доступны маршруты от клиентов SSH к серверу SSH, а также доступен маршрут от сервера SSH к серверу Radius.
- Настройте сервер SSH на сетевом устройстве, которое работает как клиент SSH.
- Настройте параметры AAA на сетевом устройстве. Когда используется режим аутентификации AAA, списки методов создаются для определения аутентификации и её типов и применяются к указанной службе или интерфейсу.

7.2.4. Аутентификация с открытым ключом SSH

7.2.4.1. Сценарий

Клиенты SSH могут использовать открытые ключи для аутентификации, а алгоритмом открытого ключа может быть RSA или DSA, как показано на Рисунке 7-4. SSH настраивается на клиенте таким образом, чтобы между клиентом SSH и сервером SSH устанавливалось безопасное соединение.



Рисунок 7-4. Топология сети для аутентификации пользователей SSH с помощью открытого ключа

7.2.4.2. Развертывание

- Чтобы реализовать аутентификацию с открытым ключом для клиента, сгенерируйте пару ключей (RSA или DSA) на клиенте, настройте открытый ключ на сервере SSH и выберите режим аутентификации с открытым ключом.
- После того, как ключ сгенерирован на клиенте, сервер SSH скопирует файл открытого ключа с клиента на флэш-память и свяжет файл с именем пользователя SSH. Каждый пользователь может быть связан с одним открытым ключом RSA и одним открытым ключом DSA.

7.2.5. Передача файлов SSH

7.2.5.1. Сценарий

Служба SCP включена на сервере, и команды SCP используются на клиенте для передачи данных на сервер, как показано на Рисунке 7-5.



Рисунок 7-5. Сетевая топология передачи файлов SSH

7.2.5.2. Развертывание

- Включите службу SCP на сервере.
- На клиенте используйте команды SCP для загрузки файлов на сервер или загрузки файлов с сервера.

7.2.6. SSH-клиентское приложение

7.2.6.1. Сценарий

Служба SSH включена на удаленном сервере SSH, а команда **ssh** используется на локальном клиенте для установки соединения SSH с сервером для безопасной передачи данных, как показано на Рисунке 7-6.



Рисунок 7-6. Сетевая топология клиентского приложения SSH

7.2.6.2. Развертывание

- Включите службу SSH на сервере.

- На клиенте запустите команду **ssh**, чтобы установить SSH-соединение с сервером для безопасной передачи данных.

7.3. Функции

7.3.1. Базовые концепты

Механизм аутентификации пользователя

- Аутентификация по паролю

Во время аутентификации по паролю клиент отправляет запрос на аутентификацию пользователя и зашифрованные имя пользователя и пароль на сервер. Сервер расшифровывает полученную информацию, сравнивает расшифрованную информацию с хранящейся на сервере, а затем возвращает сообщение об успешной или неудачной аутентификации.

- Аутентификация с открытым ключом

Во время аутентификации с открытым ключом для аутентификации клиента используются алгоритмы цифровой подписи, такие как RSA и DSA. Клиент отправляет серверу запрос на аутентификацию с открытым ключом. Этот запрос содержит информацию, включая имя пользователя, открытый ключ и алгоритм открытого ключа. Получив запрос, сервер проверяет правильность открытого ключа. В случае ошибки сервер напрямую отправляет сообщение об ошибке аутентификации. Если верно, сервер выполняет аутентификацию цифровой подписи на клиенте и возвращает сообщение, указывающее на успешную или неуспешную аутентификацию.

ПРИМЕЧАНИЕ: аутентификация с открытым ключом применима только к клиентам SSHv2.

SSH-связь

Для обеспечения безопасной связи взаимодействие между SSH-сервером и SSH-клиентом проходит следующие семь этапов:

- Настройка подключения

Сервер прослушивает на порту 22 запрос на подключение от клиента. После создания запроса на начальное соединение сокета клиент устанавливает соединение сокета TCP с сервером.

- Согласование версии

Если соединение установлено успешно, сервер отправляет клиенту пакет согласования версии. При получении пакета клиент анализирует пакет и возвращает серверу выбранную версию протокола. Сервер анализирует полученную информацию, чтобы определить, успешно ли согласование версии.

- Обмен ключами и согласование алгоритма

Если согласование версии прошло успешно, выполняется обмен ключами и согласование алгоритма. Сервер и клиент обмениваются друг с другом пакетом согласования алгоритма и определяют окончательный алгоритм на основе своих возможностей. Кроме того, сервер и клиент совместно генерируют ключ сеанса и идентификатор сеанса в соответствии с алгоритмом обмена ключами и ключом хоста, которые будут применяться для последующей аутентификации пользователя, шифрования и расшифровки данных.

- Аутентификация пользователя

После настройки зашифрованного канала клиент отправляет серверу запрос аутентификации. Сервер неоднократно проводит аутентификацию клиента до тех пор, пока аутентификация не завершится успешно или сервер не закроет соединение из-за достижения максимального числа попыток аутентификации.

- Запрос сеанса

После успешной аутентификации клиент отправляет запрос сеанса на сервер. Сервер ожидает и обрабатывает запрос клиента. После успешной обработки запроса сеанса SSH переходит к этапу сеансового взаимодействия.

- Сеанс взаимодействие

После успешной обработки запроса сеанса SSH переходит к этапу сеансового взаимодействия. Зашифрованные данные могут передаваться и обрабатываться в обоих направлениях. Клиент отправляет команду для выполнения клиенту. Сервер расшифровывает, анализирует и обрабатывает полученную команду, а затем отправляет зашифрованный результат выполнения клиенту. Клиент расшифровывает результат выполнения.

- Окончание сеанса

Когда взаимодействие между сервером и клиентом завершается, соединение сокета разрывается, и сеанс завершается.

7.3.2. Обзор

Особенность	Описание
SSH-сервер	Включите функцию SSH-сервера на сетевом устройстве, и вы сможете настроить безопасное соединение с сетевым устройством через SSH-клиент
Служба SCP	После включения службы SCP вы можете напрямую загружать файлы с сетевого устройства и загружать локальные файлы на сетевое устройство. Кроме того, все интерактивные данные зашифрованы, что обеспечивает аутентификацию и безопасность
SSH-клиент	Вы можете использовать клиент SSH на устройстве для установки безопасного соединения с сервером SSH на сетевом устройстве

7.3.3. SSH-сервер

Включите функцию SSH-сервера на сетевом устройстве, и вы сможете настроить безопасное соединение с сетевым устройством через SSH-клиент. Вы также можете отключить функцию сервера SSH, чтобы отключиться от всех клиентов SSH.

7.3.3.1. Принцип работы

Дополнительные сведения о принципе работы сервера SSH см. в разделе «SSH-связь» раздела «Базовые концепты». На практике после включения функции SSH-сервера вы можете настроить следующие параметры в соответствии с требованиями приложения:

- Версия: настройте версию SSH как SSHv1 или SSHv2 для подключения клиентов SSH.
- Время ожидания аутентификации: сервер SSH запускает таймер после получения запроса на подключение пользователя. Сервер SSH отключается от клиента либо при успешной аутентификации, либо по истечении времени ожидания аутентификации.

- Максимальное количество попыток аутентификации: SSH-сервер начинает аутентификацию клиента после получения его запроса на подключение. Если аутентификация не удалась, когда достигнуто максимальное количество попыток аутентификации пользователя, отправляется сообщение, указывающее на сбой аутентификации.
- Аутентификация с открытым ключом. Алгоритм открытого ключа может быть RSA или DSA. Он обеспечивает безопасное соединение между клиентом и сервером. Файл открытого ключа на клиенте связан с именем пользователя. Кроме того, на клиенте настраивается режим аутентификации с открытым ключом и указывается соответствующий файл закрытого ключа. Таким образом, когда клиент пытается войти на сервер, может быть реализована аутентификация с открытым ключом для установки безопасного соединения.

7.3.3.2. Связанная конфигурация

Включение SSH-сервера

По умолчанию сервер SSH отключен.

В режиме глобальной конфигурации запустите команду [**no**] **enable service ssh-server**, чтобы включить или отключить сервер SSH.

Чтобы сгенерировать ключ SSH, вам также необходимо включить сервер SSH.

Указание версии SSH

По умолчанию сервер SSH поддерживает как SSHv1, так и SSHv2, подключая либо клиентов SSHv1, либо клиентов SSHv2.

Запустите команду **ip ssh version**, чтобы настроить версию SSH, поддерживаемую сервером SSH.

Если настроен только SSHv1 или SSHv2, к SSH-серверу может быть подключен только SSH-клиент настроенной версии.

Настройка тайм-аута аутентификации SSH

По умолчанию тайм-аут аутентификации пользователя составляет 120 секунд.

Запустите команду **ip ssh time-out**, чтобы настроить тайм-аут аутентификации пользователя на сервере SSH. Используйте форму **no** команды, чтобы восстановить время ожидания по умолчанию. Сервер SSH запускает таймер после получения запроса на подключение пользователя. Если аутентификация не завершается успешно до истечения времени ожидания, аутентификация завершается с ошибкой.

Настройка максимального количества попыток аутентификации SSH

По умолчанию максимальное количество попыток аутентификации пользователя равно 3.

Запустите команду **ip ssh authentication-retries**, чтобы настроить максимальное количество попыток аутентификации пользователя на сервере SSH. Используйте форму **no** команды, чтобы восстановить количество попыток аутентификации пользователя по умолчанию. Если аутентификация по-прежнему не проходит успешно, когда достигнуто максимальное количество попыток аутентификации пользователя, аутентификация пользователя не удалась.

Указание режима шифрования SSH

По умолчанию режим шифрования, поддерживаемый сервером SSH, является Compatible (совместимым), то есть поддерживает цепочку блоков шифрования (CBC), счетчик (CTR) и другие режимы шифрования.

Запустите команду **ip ssh cipher-mode**, чтобы настроить режим шифрования, поддерживаемый сервером SSH. Используйте форму **no** команды, чтобы восстановить режим шифрования по умолчанию, поддерживаемый сервером SSH.

Указание алгоритма аутентификации сообщений SSH

По умолчанию сервер SSH поддерживает следующие алгоритмы аутентификации сообщений: (1) для SSHv1 алгоритм не поддерживается; (2) Для SSHv2 поддерживаются четыре алгоритма, включая MD5, SHA1, SHA1-96 и MD5-96.

Запустите команду **ip ssh hmac-algorithm**, чтобы настроить алгоритм аутентификации сообщений, поддерживаемый сервером SSH. Используйте форму **no** команды, чтобы восстановить алгоритм идентификации сообщений по умолчанию, поддерживаемый сервером SSH.

Настройка поддержки алгоритма обмена ключами Диффи-Хеллмана (DH) на сервере SSH

По умолчанию сервер QTECH SSHv2 поддерживает diffie-hellman-group-exchange-sha1, diffie-hellmangroup14-sha1 и diffie-hellman-group1-sha1 для обмена ключами, в то время как сервер SSHv1 не поддерживает ничего. Запустите команду **ip ssh key-exchange**, чтобы настроить поддержку Диффи-Хеллмана на сервере SSH. Используйте команду **no ip ssh key-exchange**, чтобы восстановить настройки по умолчанию.

Настройка фильтрации ACL для SSH-сервера

По умолчанию фильтрация ACL не выполняется для всех подключений к SSH-серверу.

Запустите команду **{ip | ipv6} ssh access-class** для выполнения фильтрации ACL для всех подключений к SSH-серверу. Запустить команду **no {ip | ipv6} ssh access-class** для восстановления настроек по умолчанию.

Включение аутентификации с открытым ключом на сервере SSH

Запустите команду **ip ssh peer**, чтобы связать файл открытого ключа на клиенте с именем пользователя. Когда клиент аутентифицируется при входе в систему, файл открытого ключа указывается на основе имени пользователя.

7.3.4. Служба SCP

Сервер SSH предоставляет службу SCP для реализации безопасной передачи файлов между сервером и клиентом.

7.3.4.1. Принцип работы

- SCP — это протокол, поддерживающий онлайн-передачу файлов. Он работает на порту 22 на основе протокола BSC RCP, тогда как RCP обеспечивает функции шифрования и аутентификации на основе протокола SSH. RCP реализует передачу файлов, а SSH реализует аутентификацию и шифрование.
- Предположим, что служба SCP включена на сервере. Когда вы используете клиент SCP для загрузки или скачивания файлов, клиент SCP сначала анализирует параметры команды, устанавливает соединение с удаленным сервером и запускает другой процесс SCP на основе этого соединения. Этот процесс может работать в режиме источника или приемника. (Процесс, работающий в исходном режиме, является поставщиком данных. Процесс, работающий в режиме приемника, является получателем данных.) Процесс, работающий в исходном режиме, считывает и отправляет файлы на peer end-узел через соединение SSH. Процесс, работающий в режиме приемника, получает файлы через соединение SSH.

7.3.4.2. Связанная конфигурация

Включение сервера SCP

По умолчанию функция сервера SCP отключена.

Запустите команду **ip scp server enable**, чтобы включить функцию сервера SCP на сетевом устройстве.

7.3.5. SSH-клиент

Клиент SSH используется для установки безопасного соединения с удаленным сетевым устройством, на котором работает сервер SSH.

7.3.5.1. Принцип работы

Дополнительные сведения о принципе работы клиента SSH см. в разделе «SSH-связь» раздела «Базовые концепты».

7.3.5.2. Связанная конфигурация

Указание исходного интерфейса клиента SSH

По умолчанию исходный адрес SSH-пакетов ищется на основе адреса получателя.

Запустите команду **ip ssh source-interface** *interface-name*, чтобы указать исходный интерфейс клиента SSH.

Установление сеанса с сервером SSH

Запустите команду **ssh**, чтобы войти на удаленное устройство, которое поддерживает сервер SSH.

Восстановление установленной сессии SSH

Запустите команду **ssh-session** *session-id*, чтобы восстановить установленный сеанс SSH.

Отключение приостановленного сеанса SSH

Запустите команду **disconnect ssh-session** *session-id*, чтобы отключить указанный сеанс SSH.

7.3.6. SCP-клиент

Клиент SCP используется для поддержки передачи файлов с удаленным сетевым устройством, на котором включен сервер SCP.

7.3.6.1. Принцип работы

SCP — это протокол, поддерживающий онлайн-передачу файлов. Он работает на порту 22 на основе BSD RCP, в то время как RCP обеспечивает функции шифрования и аутентификации на основе протокола SSH. RCP реализует передачу файлов, а SSH реализует аутентификацию и шифрование.

Когда вы используете клиент SCP для загрузки или скачивания файлов, клиент SCP сначала анализирует параметры команды, устанавливает соединение с удаленным сервером и запускает другой процесс SCP на основе этого соединения. Этот процесс может работать в исходном режиме или режиме приемника. Процесс выступает в качестве поставщика данных в исходном режиме и считывает, и отправляет файлы на peer end-узел через соединение SSH, а в режиме приемника выступает в качестве получателя данных и получает файлы через соединение SSH.

7.3.6.2. Связанная конфигурация

Указание исходного интерфейса клиента SCP

По умолчанию настройте IP-адрес исходного интерфейса в качестве исходного адреса в SSH-пакетах.

Запустите команду **ip scp client source-interface** *interface-name*, чтобы указать интерфейс клиента SCP.

Установление соединения с SCP-сервером через SCP-клиент для реализации передачи файлов

Запустите команду **scp**, чтобы реализовать передачу файлов с помощью SSH-сервера.

7.4. Конфигурация

Конфигурация	Описание и команда	
Настройка SSH-сервера	Обязательно включить сервер SSH	
	enable service ssh-server	Включает SSH-сервер
	disconnect ssh[vty] *session-id*	Отключает установленный сеанс SSH
	crypto key generate {rsa|dsa}	Генерирует SSH-ключ
	ip ssh version {1|2}	Указывает версию SSH
	ip ssh time-out *time*	Настраивает время ожидания аутентификации SSH
	ip ssh authentication-retries *retry times*	Настраивает максимальное количество попыток аутентификации SSH
	ip ssh cipher-mode{cbc | ctr | others }	Указывает режим шифрования SSH
	ip ssh hmac-algorithm{md5 | md5-96 | sha1 | sha1-96}	Задает алгоритм идентификации сообщения SSH
	ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }	Настраивает поддержку Диффи-Хеллман на SSH-сервере

Конфигурация	Описание и команда	
Настройка SSH-сервера	**{ip | ipv6} ssh access-class** { *access-list-number* | *access-listname* }	Включает фильтрацию ACL для SSH-сервера
	ip ssh peer test public-key rsa flash :*rsa.pub*	Связывает файл открытого ключа RSA с пользователем
	ip ssh peer test public-key dsa flash:*dsa.pub*	Связывает файл открытого ключа DSA с пользователем
Настройка службы SCP	Обязательный	
	ip scp server enable	Включает сервер SCP
Настройка SSH-клиента	(Опционально) Используется для установки безопасного соединения с удаленным сетевым устройством, поддерживающим SSH-сервер	
	ip ssh source-interface *interface-name*	Указывает исходный интерфейс клиента SSH
	ssh [**oob**] [**-v** {**1** | **2** }][**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }] [**-l** *username*][**-m** {**hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** }] [**-p** *port-num*]{ *ip-addr*| *hostname*}[**via** *mgmt name*][**/source** {**ip***A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name*}] [**/vrf** *vrf-name*]	Устанавливает зашифрованный сеанс с удаленным сетевым устройством

7.4.1. Настройка SSH-сервера

7.4.1.1. Эффект конфигурации

- Включите функцию SSH-сервера на сетевом устройстве, чтобы можно было установить безопасное соединение с удаленным сетевым устройством через SSH-клиент. Все интерактивные данные шифруются перед передачей, обеспечивая аутентификацию и безопасность.
- Вы можете использовать различные режимы аутентификации пользователей SSH, включая аутентификацию по локальному паролю, аутентификацию AAA и аутентификацию с открытым ключом.
- Вы можете сгенерировать или удалить ключ SSH.
- Вы можете указать версию SSH.
- Вы можете настроить время ожидания аутентификации SSH.

- Вы можете настроить максимальное количество попыток аутентификации SSH.
- Вы можете указать режим шифрования SSH.
- Вы можете указать алгоритм аутентификации сообщений SSH.
- Вы можете указать фильтрацию ACL для SSH-сервера.

7.4.1.2. Примечания

- Предварительным условием настройки устройства в качестве SSH-сервера является бесперебойная связь в сети, в которой находится устройство, и администратор может получить доступ к интерфейсу управления устройством для настройки соответствующих параметров.
- Команда **no crypto key generate** не существует. Вам нужно запустить команду **crypto key zeroize**, чтобы удалить ключ.
- Модуль SSH не поддерживает горячее резервирование. Таким образом, для продуктов, поддерживающих горячее резервирование в модулях супервизора, если файл ключа SSH не существует в новом активном модуле после отработки отказа, необходимо выполнить команду **crypto key generate**, чтобы повторно сгенерировать ключ перед использованием SSH.

7.4.1.3. Шаги настройки

Включение SSH-сервера

- Обязательный.
- По умолчанию сервер SSH отключен. В режиме глобальной конфигурации включите сервер SSH и сгенерируйте ключ SSH, чтобы состояние сервера SSH изменилось на ENABLE.

Указание версии SSH

- Опционально.
- По умолчанию сервер SSH поддерживает SSHv1 и SSHv2, подключая клиентов SSHv1 или SSHv2. Если настроен только SSHv1 или SSHv2, к SSH-серверу может быть подключен только SSH-клиент настроенной версии.

Настройка тайм-аута аутентификации SSH

- Опционально.
- По умолчанию тайм-аут аутентификации SSH составляет 120 секунд. При необходимости вы можете настроить тайм-аутм аутентификации пользователя. Значение находится в диапазоне от 1 до 120. Единицей измерения является секунда.

Настройка максимального количества попыток аутентификации SSH

- Опционально.
- Настройте максимальное количество повторных попыток аутентификации SSH, чтобы предотвратить неправомерное поведение, такое как злонамеренное предположение. По умолчанию максимальное количество попыток аутентификации SSH равно 3, то есть пользователю разрешено ввести имя пользователя и пароль три раза для аутентификации. При необходимости вы можете настроить максимальное количество повторных попыток. Значение варьируется от 0 до 5.

Указание режима шифрования SSH

- Опционально.

- Укажите режим шифрования, поддерживаемый сервером SSH. По умолчанию режим шифрования, поддерживаемый SSH-сервером, является Compatible, то есть поддерживает CBC, CTR и другие режимы шифрования.

Указание алгоритма аутентификации сообщений SSH

- Опционально.
- Укажите алгоритм аутентификации сообщений, поддерживаемый сервером SSH. По умолчанию сервер SSH поддерживает следующие алгоритмы аутентификации сообщений: (1) для SSHv1 алгоритм не поддерживается; (2) Для SSHv2 поддерживаются четыре алгоритма, включая MD5, SHA1, SHA1-96 и MD5-96.

Настройка фильтрации ACL для SSH-сервера

- Опционально.
- Установите фильтрацию ACL SSH-сервера. По умолчанию фильтрация ACL выполняется не для всех подключений к SSH-серверу. В соответствии с потребностями установите фильтрацию ACL для выполнения для всех подключений к SSH-серверу.

Включение аутентификации с открытым ключом для пользователей SSH

- Опционально.
- Только SSHv2 поддерживает аутентификацию на основе открытого ключа. Эта конфигурация связывает файл открытого ключа на клиенте с именем пользователя. Когда клиент аутентифицируется при входе в систему, файл открытого ключа указывается на основе имени пользователя.

7.4.1.4. Проверка

- Запустите команду **show ip ssh**, чтобы отобразить текущую версию SSH, время ожидания аутентификации и максимальное количество попыток аутентификации сервера SSH.
- Запустите команду **show crypto key mypubkey**, чтобы отобразить общедоступную информацию об открытом ключе и проверить, был ли он сгенерирован.
- Настройте режим входа в систему с аутентификацией с открытым ключом на клиенте SSH и укажите файл приватного ключа. Проверьте, можете ли вы успешно войти на сервер SSH из клиента SSH. Если да, файл открытого ключа на клиенте успешно связывается с именем пользователя, и проверка подлинности с открытым ключом завершается успешно.

7.4.1.5. Связанные команды

Включение SSH-сервера

Команда	**enable service ssh-server**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы отключить сервер SSH, запустите команду **no enable service ssh-server** в режиме глобальной конфигурации. После выполнения этой команды состояние SSH-сервера изменится на DISABLE

Отключение установленного сеанса SSH

Команда	**disconnect ssh[vty]** *session-id*
Описание параметров	**vty**: указывает на установленный сеанс виртуального терминала телетайпа (VTY). *session-id*: указывает идентификатор установленного сеанса SSH. Значение варьируется от 0 до 35
Командный режим	Привилегированный режим EXEC
Руководство по использованию	Укажите идентификатор сеанса SSH, чтобы отключить установленный сеанс SSH. В качестве альтернативы укажите идентификатор сеанса VTY, чтобы отключить указанный сеанс SSH. Только сессия SSH может быть отключена

Генерация SSH-ключа

Команда	**crypto key generate {rsa|dsa}**
Описание параметров	**rsa**: генерирует ключ RSA. **dsa**: генерирует ключ DSA
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Команда **no crypto key generate** не существует. Вам нужно запустить команду **crypto key zeroize**, чтобы удалить ключ. SSHv1 использует ключ RSA, тогда как SSHv2 использует ключ RSA или DSA. Если сгенерирован ключ RSA, поддерживаются как SSHv1, так и SSHv2. Если сгенерирован только ключ DSA, только SSHv2 может использовать этот ключ

Указание версии SSH

Команда	**ip ssh version {1|2}**
Описание параметров	**1**: указывает, что сервер SSH получает только запросы на подключение, отправленные клиентами SSHv1. **2**: указывает, что сервер SSH получает только запросы на подключение, отправленные клиентами SSHv2
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Запустите команду **no ip ssh version**, чтобы восстановить настройки по умолчанию. По умолчанию сервер SSH поддерживает как SSHv1, так и SSHv2

Настройка времени ожидания аутентификации SSH

Команда	**ip ssh time-out** *time*
Описание параметров	*time*: указывает время ожидания аутентификации SSH. Значение находится в диапазоне от 1 до 120. Единицей измерения является секунда
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **no ip ssh time-out**, чтобы восстановить время ожидания аутентификации SSH по умолчанию, равное 120 с

Настройка максимального количества попыток аутентификации SSH

Команда	**ip ssh authentication-retries** *retry times*
Описание параметров	*retry times*: указывает максимальное количество попыток аутентификации пользователя. Значение варьируется от 0 до 5
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **no ip ssh authentication-retries**, чтобы восстановить количество попыток аутентификации пользователя по умолчанию, равное 3

Указание режима шифрования SSH

Команда	**ip ssh cipher-mode {cbc | ctr | others }**
Описание параметров	**cbc**: устанавливает режим шифрования, поддерживаемый сервером SSH, на режим CBC. Соответствующие алгоритмы включают DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC и Blowfish-CBC. **ctr**: устанавливает режим шифрования, поддерживаемый сервером SSH, в режим CTR. Соответствующие алгоритмы включают AES128-CTR, AES192-CTR и AES256-CTR. **others**: устанавливает режим шифрования, поддерживаемый сервером SSH, на другие. Соответствующий алгоритм — RC4
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Эта команда используется для настройки режима шифрования, поддерживаемого сервером SSH. На устройствах QTECH сервер SSHv1 поддерживает алгоритмы шифрования DES-CBC, 3DES-CBC и Blowfish-CBC; сервер SSHv2 поддерживает алгоритмы шифрование AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC и RC4. Эти алгоритмы можно сгруппировать в три режима шифрования: CBC, CTR и others. Поскольку криптография постоянно развивается, утверждается, что алгоритмы шифрования в режимах CBC и others могут быть расшифрованы за ограниченный период времени. Поэтому организации или компании с высокими требованиями к безопасности могут установить режим шифрования, поддерживаемый сервером SSH, на CTR, чтобы повысить уровень безопасности сервера SSH

Указание алгоритма аутентификации сообщений SSH

Команда	**ip ssh hmac-algorithm {md5 | md5-96 | sha1 | sha1-96}**
Описание параметров	**md5**: указывает, что алгоритм аутентификации сообщений, поддерживаемый сервером SSH, — MD5. **md5-96**: указывает, что сервер SSH поддерживает алгоритм аутентификации сообщений MD5-96. **sha1**: указывает, что сервер SSH поддерживает алгоритм аутентификации сообщений SHA1. **sha1-96**: указывает, что сервер SSH поддерживает алгоритм аутентификации сообщений SHA1-96
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки алгоритма аутентификации сообщений, поддерживаемого сервером SSH. На устройствах QTECH сервер SSHv1 поддерживает любой алгоритм аутентификации сообщений; сервер SSHv2 поддерживает алгоритмы аутентификации сообщений MD5, SHA1, SHA1-96 и MD5-96. При необходимости вы можете выбрать алгоритмы аутентификации сообщений, поддерживаемые SSH-сервером

Настройка поддержки алгоритма обмена ключами DH на сервере SSH

Команда	**ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }**
Описание параметров	**dh_group_exchange_sha1**: указывает конфигурацию diffie-hellman-group-exchange-sha1 для обмена ключами. Ключ имеет 2048 байт, которые нельзя редактировать. **dh_group14_sha1**: указывает конфигурацию diffie-hellman-group14-sha1 для обмена ключами. Ключ имеет размер 2048 байт. **dh_group1_sha1**: указывает конфигурацию diffie-hellman-group1-sha1 для обмена ключами. Ключ имеет размер 1024 байта
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для настройки метода обмена ключами DH в SSH. Сервер QTECH SSHv1 не поддерживает метод обмена ключами DH, в то время как сервер SSHv2 поддерживает diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1 и diffie-hellman-group1-sha1 для обмена ключами

Настройка фильтрации ACL для SSH-сервера

Команда	**{ip | ipv6} ssh access-class** { *access-list-number* | *access-list-name* }
Описание параметров	*access-list-number*: указывает номер ACL, диапазон номеров можно настроить. Стандартные диапазоны номеров ACL — от 1 до 99 и от 1300 до 1999. Расширенные диапазоны номеров ACL — от 100 до 199 и от 2000 до 2699. Поддерживаются только адреса IPv4. *access-list-name*: указывает имя ACL. Поддерживаются адреса IPv4 и IPv6
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы выполнить фильтрацию ACL для всех подключений к серверу SSH. В режиме line фильтрация ACL выполняется только для определенных строк. Однако правила фильтрации ACL для SSH действуют для всех соединений SSH

Настройка аутентификации с открытым ключом RSA

Команда	**ip ssh peer** *test* **public-key rsaflash**:*rsa.pub*
Описание параметров	*test*: указывает имя пользователя. **rsa**: указывает, что тип открытого ключа — RSA. *rsa.pub*: указывает имя файла открытого ключа
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки файла открытого ключа RSA, связанного с пользовательским тестом. Только SSHv2 поддерживает аутентификацию на основе открытого ключа. Эта команда связывает файл открытого ключа на клиенте с именем пользователя. Когда клиент аутентифицируется при входе в систему, файл открытого ключа указывается на основе имени пользователя

Настройка аутентификации с открытым ключом DSA

Команда	**ip ssh peer** *test* **public-key dsaflash**:*dsa.pub*
Описание параметров	*test*: указывает имя пользователя. **dsa**: указывает, что тип открытого ключа — DSA. *dsa.pub*: указывает имя файла открытого ключа
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки файла ключа DSA, связанного с пользовательским тестом. Только SSHv2 поддерживает аутентификацию на основе открытого ключа. Эта команда связывает файл открытого ключа на клиенте с именем пользователя. Когда клиент аутентифицируется при входе в систему, файл открытого ключа указывается на основе имени пользователя

7.4.1.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации описываются только конфигурации, связанные с SSH.

Генерация открытого ключа на SSH-сервере

Шаги настройки	Запустите команду **crypto key generate { rsa | dsa }** для создания открытого ключа RSA для сервера

SSH-сервер	QTECH#configure terminal QTECH(config)# crypto key generate rsa Choose the size of the rsa key modulus in the range of 512 to 2048 and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: Если генерация ключа RSA прошла успешно, отображается следующая информация: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Если генерация ключа RSA не удалась, отображается следующая информация: % Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]
Проверка	Запустите команду **show crypto key mypubkey rsa**, чтобы отобразить общедоступную информацию о ключе RSA. Если общедоступная информация о ключе RSA существует, ключ RSA был сгенерирован
SSH-сервер	QTECH(config)#show crypto key mypubkey rsa % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA1 private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU 8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFlKDj1j 0dKBcCfN tr0r/CT+ cs5tlGKV S0ICGifz oB+pYaE= % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEAAQAAAHJfLwKnzOgO F3RlKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc

	w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISgIfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4liQuTIL HRgtbyEYXCFaaxU=

Указание версии SSH

Шаги настройки	Запустите команду **ip ssh version { 1 | 2 }**, чтобы установить версию, поддерживаемую сервером SSH, на SSHv2
SSH-сервер	QTECH#configure terminal QTECH(config)#ip ssh version 2
Проверка	Запустите команду **show ip ssh**, чтобы отобразить версию SSH, поддерживаемую в настоящее время сервером SSH
SSH-сервер	QTECH(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled

Настройка тайм-аута аутентификации SSH

Шаги настройки	Запустите команду **ip ssh time-out** *time*, чтобы установить тайм-аут аутентификации SSH равным 100 с
SSH-сервер	QTECH#configure terminal QTECH(config)#ip sshtime-out100
Проверка	Запустите команду **show ip ssh**, чтобы отобразить настроенный тайм-аут аутентификации SSH
SSH-сервер	QTECH(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Настройка максимального количества попыток аутентификации SSH

Шаги настройки	Запустите команду **ip ssh authentication-retries** *retry times*, чтобы установить максимальное количество попыток аутентификации пользователя на сервере SSH равным 2

SSH-сервер	QTECH#configure terminal QTECH(config)#ip ssh authentication-retries 2
Проверка	Запустите команду **show ip ssh**, чтобы отобразить настроенное максимальное количество попыток аутентификации
SSH-сервер	QTECH(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Указание режима шифрования SSH

Шаги настройки	Запустите команду **ip ssh cipher-mode {cbc | ctr | others }** для установки режима шифрования, поддерживаемого сервером SSH, на CTR
SSH-сервер	QTECH#configure terminal QTECH(config)# ip ssh cipher-mode ctr
Проверка	Выберите режим шифрования CTR на клиенте SSH и проверьте, можете ли вы успешно войти на сервер SSH с клиента SSH

Указание алгоритма аутентификации сообщений SSH

Шаги настройки	Запустите команду **ip ssh hmac-algorithm {md5 | md5-96 | sha1 | sha1-96 }**, чтобы установить алгоритм аутентификации сообщений, поддерживаемый сервером SSH, на SHA1
SSH-сервер	QTECH#configure terminal QTECH(config)# ip ssh hmac-algorithmsha1
Проверка	Выберите алгоритм аутентификации сообщений SHA1 на клиенте SSH и проверьте, можете ли вы успешно войти на сервер SSH с клиента SSH

Настройка поддержки алгоритма обмена ключами DH на сервере SSH

Шаги настройки	Запустите команду **ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 },** чтобы настроить метод обмена ключами на SSH-сервере
SSH-сервер	QTECH# configure terminal QTECH(config)# ip ssh key-exchange dh_group14_sha1

Проверка	Выберите diffie-hellman-group14-sha1 на клиентском терминале и проверьте, выполнен ли успешный вход в систему

Настройка аутентификации с открытым ключом

Шаги настройки	Запустите команду **ip ssh peer** *username* **public-key** { **rsa | dsa**}*filename*, чтобы связать файл открытого ключа клиента с именем пользователя. Когда клиент аутентифицируется при входе в систему, файл открытого ключа (например, RSA) указывается на основе имени пользователя
SSH-сервер	QTECH#configure terminal QTECH(config)# ip ssh peer test public-key rsaflash:rsa.pub
Проверка	Настройте режим входа в систему с аутентификацией с открытым ключом на клиенте SSH и укажите файл приватного ключа. Проверьте, можете ли вы успешно войти на сервер SSH из клиента SSH. Если да, файл открытого ключа на клиенте успешно связывается с именем пользователя, аутентификация с открытым ключом завершается успешно

Настройка управления устройствами SSH

Сценарий:



Рисунок 7-7.

Вы можете использовать SSH для управления устройствами при условии, что функция сервера SSH включена. По умолчанию эта функция отключена. Компонент Telnet, входящий в состав Windows, не поддерживает SSH. Поэтому необходимо использовать стороннее клиентское программное обеспечение. В настоящее время хорошо совместимое клиентское программное обеспечение включает PuTTY, Linux и SecureCRT. Далее в качестве примера используется PuTTY, чтобы представить конфигурации клиента SSH.

Шаги настройки	• Запустите программу PuTTY. • На вкладке параметров **Session** в PuTTY введите IP-адрес хоста **192.168.23.122** и номер порта SSH **22** и выберите тип подключения **SSH**. • На вкладке параметров **SSH** в PuTTY выберите предпочтительную версию протокола SSH **2**. • На вкладке параметров **SSH authentication** в PuTTY выберите метод аутентификации **Attempt "keyboard-interactive" auth**. • Нажмите **Open**, чтобы подключиться к SSH-сервер. • Введите правильное имя пользователя и пароль, чтобы войти в интерфейс входа в терминал

SSH-клиент

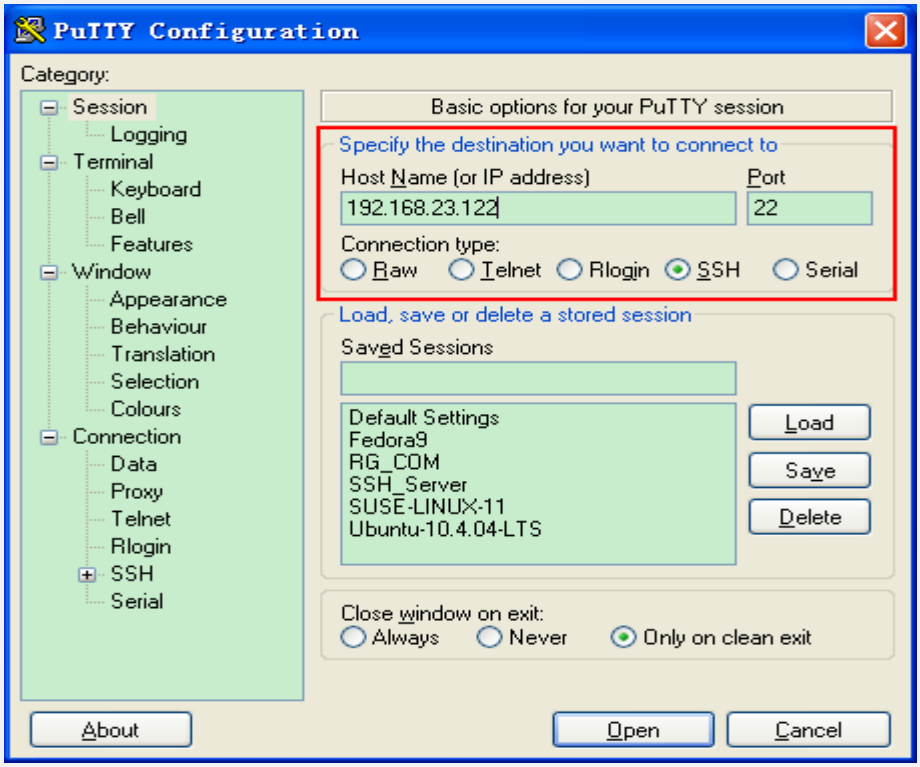


Рисунок 7-8.

Host Name (или **IP address**) указывает IP-адрес хоста, на который необходимо войти. В этом примере IP-адрес — **192.168.23.122**. **Port** указывает идентификатор порта 22, то есть идентификатор порта по умолчанию, прослушиваемый SSH. **Connection type – SSH**.

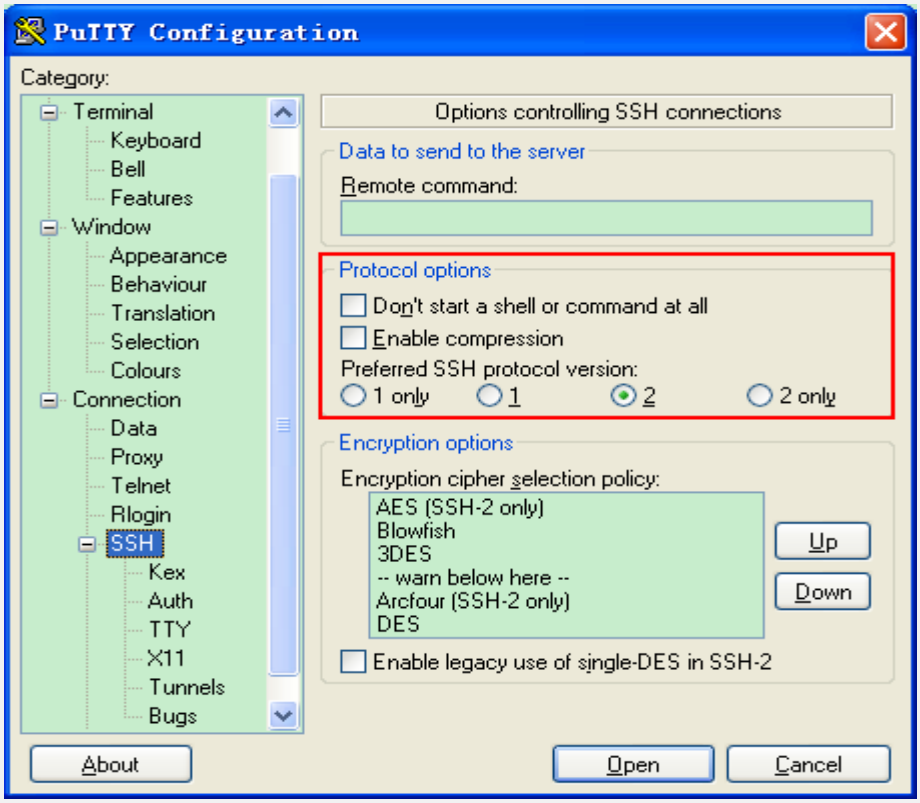


Рисунок 7-9.

Как показано Рисунке 7-9, выберите **2** в качестве предпочтительной версии протокола SSH на панели **Protocol options**, поскольку для входа используется SSHv2.

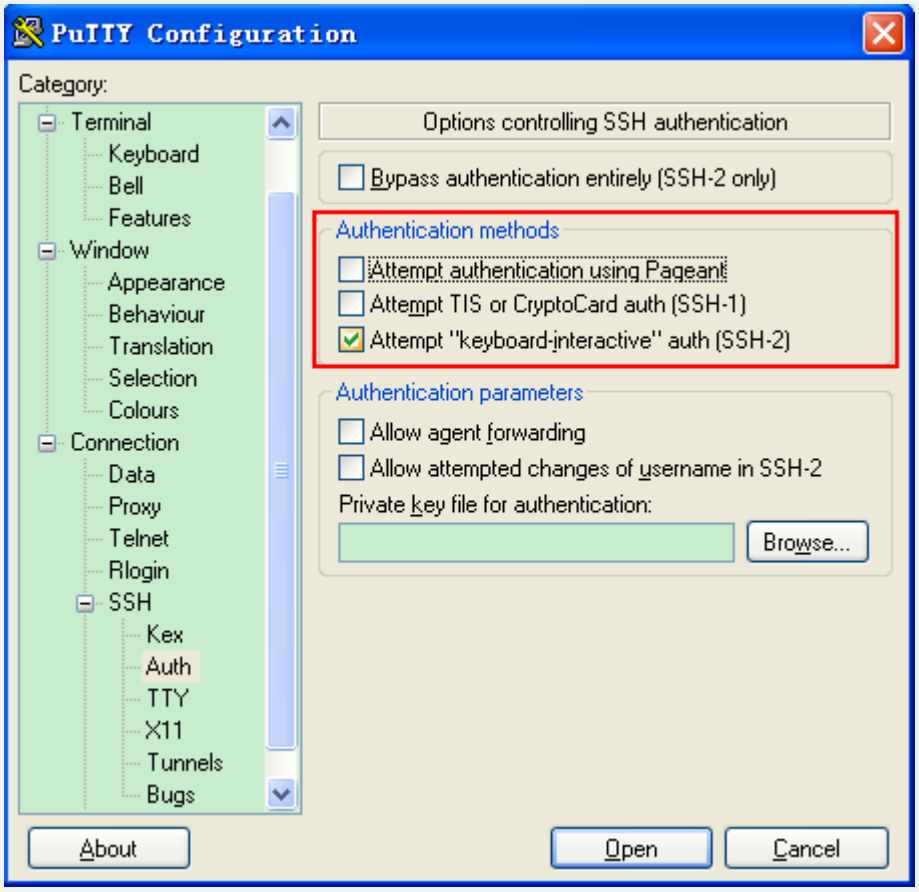


Рисунок 7-10.

Как показано на Рисунке 7-10, выберите **Attempt "keyboard-interactive" auth** в качестве метода аутентификации для поддержки аутентификации на основе имени пользователя и пароля.

Затем нажмите **Open**, чтобы подключиться к настроенному узлу сервера, как показано на Рисунке 7-11.



Рисунок 7-11.

Окно **PuTTY Security Alert** указывает, что вы входите в клиент сервера 192.168.23.122, и спрашивает вас, следует ли получить ключ, отправленный с сервера.

Если вы выберете **Yes**, появится диалоговое окно входа в систему, как показано на Рисунке 7-12.

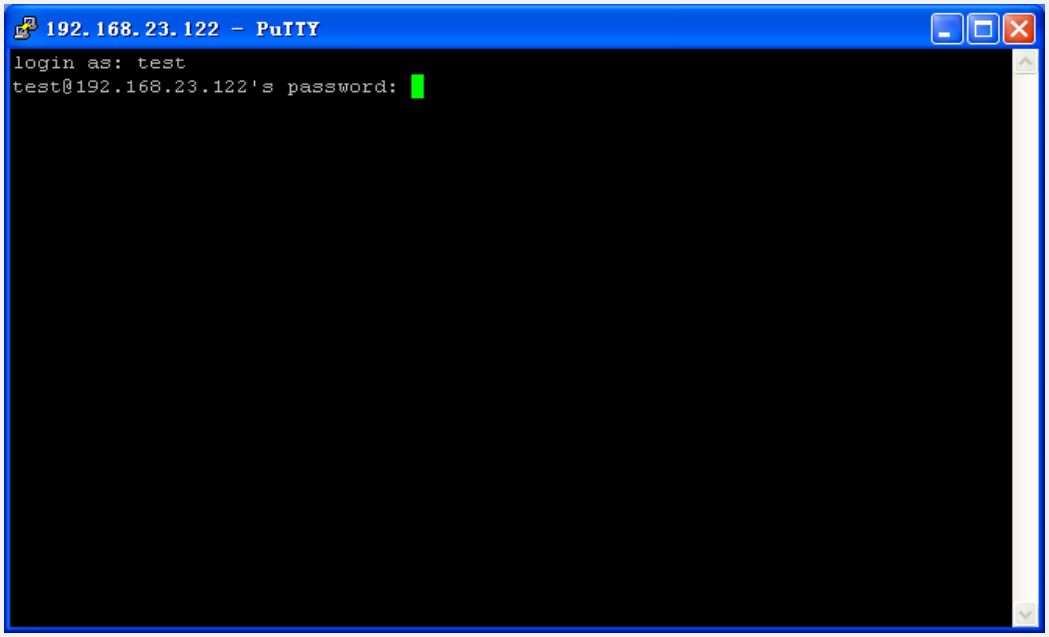


Рисунок 7-12.

Введите правильное имя пользователя и пароль, и вы сможете войти в интерфейс терминала SSH, как показано на Рисунке 7-13.

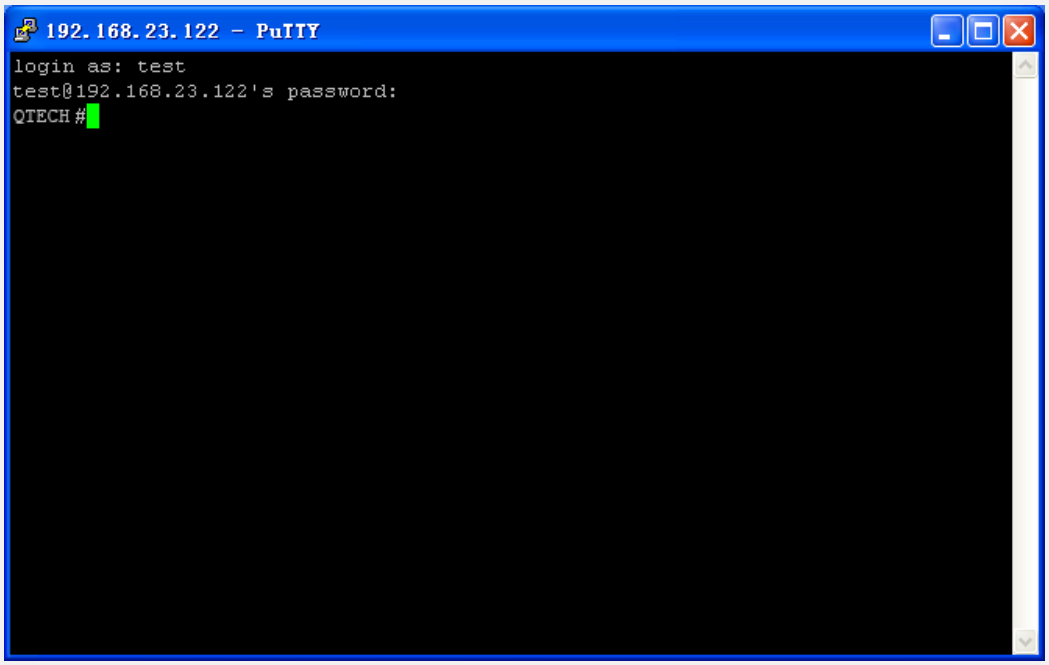


Рисунок 7-13

Проверка	Запустите командуи **show ip ssh** для отображения конфигураций, которые в настоящее время действуют на сервере SSH. Запустите команду **show ssh** для отображения информации о каждом установленном SSH-соединении
	QTECH#show ip ssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 QTECH#show ssh Connection Version Encryption Hmac State Username 0 2.0 aes256-cbc hmac-sha1 Session started test

Настройка аутентификации по локальной учетной записи SSH

Сценарий:

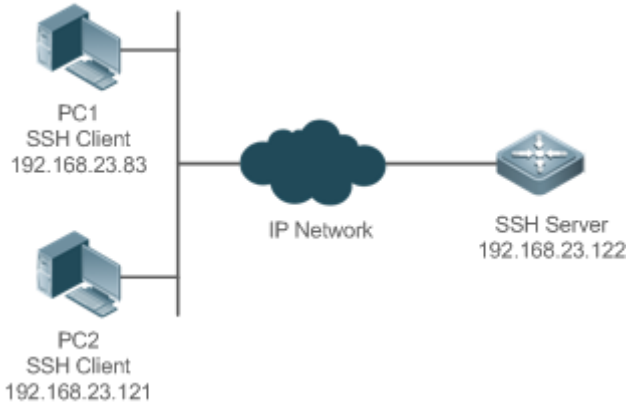


Рисунок 7-14.

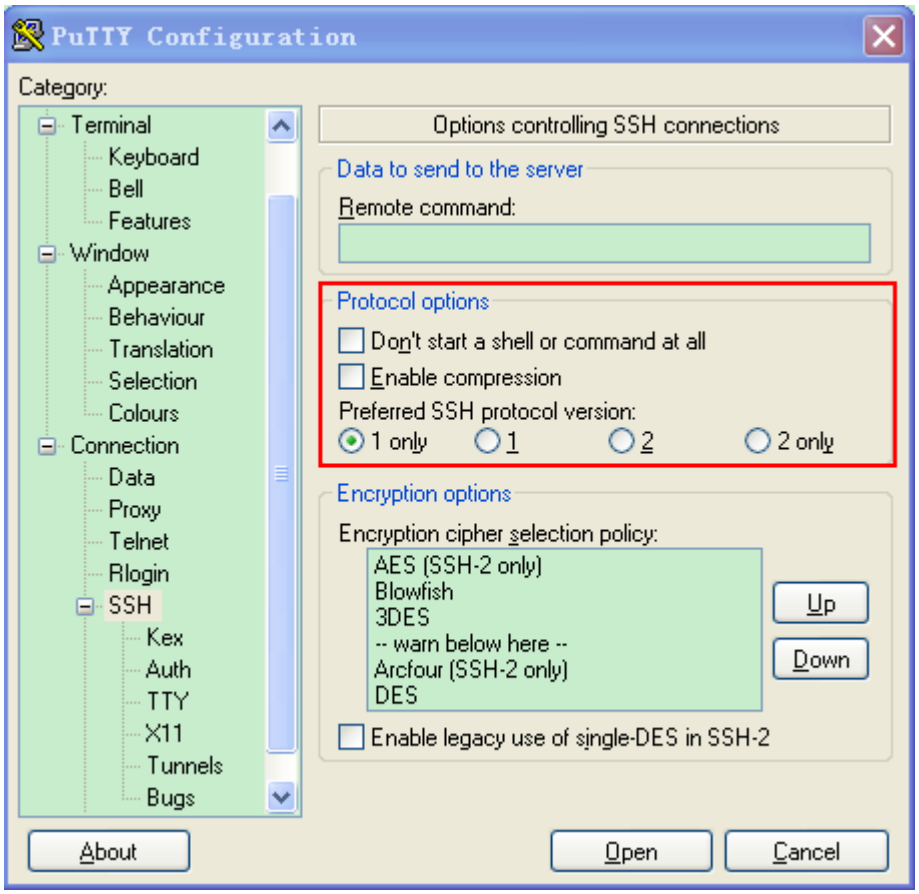
Пользователи SSH могут использовать пароль локальной учетной записи для аутентификации пользователя, как показано на Рисунке 7-14. Для обеспечения безопасности обмена данными ПК 1 и ПК 2 работают как клиенты SSH и используют протокол SSH для входа на сетевое устройство, на котором включен сервер SSH. Требования следующие:

Пользователи SSH используют режим аутентификации по паролю локальной учетной записи.

Пять строк включая строки 0 и 4, активируются одновременно. Пароль для входа «passzero» для строки 0 и «pass» для остальных строк. Можно использовать любое имя пользователя.

Шаги настройки	Настройте SSH-сервер следующим образом: • Включите функцию сервера SSH глобально. По умолчанию сервер SSH поддерживает две версии SSH: SSHv1 и SSHv2. • Настройте ключ. С помощью этого ключа SSH-сервер расшифровывает зашифрованный пароль, полученный от SSH-клиента, сравнивает расшифрованный открытый текст с

	паролем, хранящимся на сервере, и возвращает сообщение об успешной или неудачной аутентификации. SSHv1 использует ключ RSA, тогда как SSHv2 использует ключ RSA или DSA. • Настройте IP-адрес интерфейса FastEthernet 0/1 на сервере SSH. Клиент SSH подключается к серверу SSH на основе этого IP-адреса. Маршрут от клиента SSH к серверу SSH доступен. Настройте клиент SSH следующим образом: • Доступно разнообразное клиентское программное обеспечение SSH, включая PuTTY, Linux и SecureCRT. В этом документе PuTTY используется в качестве примера для объяснения метода настройки клиента SSH. Дополнительные сведения о методе настройки см. в разделе «Шаги настройки»
SSH-сервер	Перед настройкой функции, связанной с SSH, убедитесь, что маршрут от пользователя SSH к сетевому сегменту сервера SSH доступен. Конфигурации IP-адреса интерфейса показаны на Рисунке 7-15. Подробные процедуры настройки IP-адресов и маршрутов опущены. QTECH(config)# enable service ssh-server QTECH(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] QTECH(config)#interface fastEthernet0/1 QTECH(config-if-fastEthernet0/1)#ip address 192.168.23.122 255.255.255.0 QTECH(config-if-fastEthernet0/1)#exit QTECH(config)#line vty 0 QTECH(config-line)#password passzero QTECH(config-line)#privilege level 15 QTECH(config-line)#login QTECH(config-line)#exit QTECH(config)#line vty1 4 QTECH(config-line)#password pass QTECH(config-line)#privilege level 15 QTECH(config-line)#login QTECH(config-line)#exit

SSH-клиент (ПК1/ПК2)	 Рисунок 7-15. Установите IP-адрес и идентификатор порта SSH-сервера. Как показано в топологии сети, IP-адрес сервера — 192.168.23.122, а идентификатор порта — 22 (дополнительные сведения о методе настройки см. в разделе «Пример конфигурации» в «Настройка управления устройствами SSH»). Нажмите **Open**, чтобы запустить SSH-сервер. Поскольку текущий режим аутентификации не требует имени пользователя, вы можете ввести любое имя пользователя, но не можете оставить его неуказанным. (В этом примере имя пользователя — «anyname».)
Проверка	• Запустите команду **show running-config** для отображения текущих конфигураций. • Убедитесь, что конфигурации клиента SSH верны
SSH-сервер	QTECH#show running-config Building configuration… ! enable secret 5 1eyy2$xs28FDw4s2q0tx97 enable service ssh-server ! interface fastEthernet0/1

```
ip address 192.168.23.122 255.255.255.0
!
line vty 0
privilege level 15
login
password passzero
line vty 1 4
privilege level 15
login
password pass
!
end
```

SSH-клиент

Установите соединение и введите правильный пароль. Пароль для входа «passzero» для строки 0 и «pass» для остальных строк. Затем отображается интерфейс работы SSH-сервера, как показано на Рисунке 7-16.

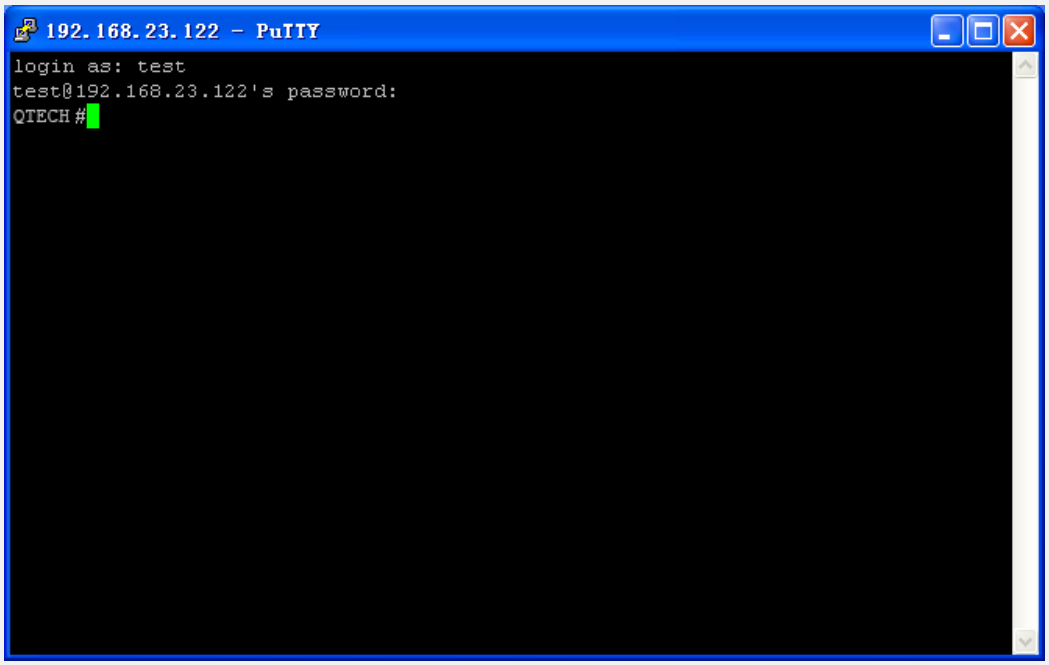


Рисунок 7-16.

```
QTECH#show users
Line            User      Host(s)            Idle         Location
--------------- --------- ------------------ ---------- -------------
* 0 con 0       ---       idle               00:00:00     ---
1 vty 0         ---       idle               00:08:02     192.168.23.83
2 vty 1         ---       idle               00:00:58     192.168.23.121
```

Настройка аутентификации AAA пользователей SSH

Сценарий:

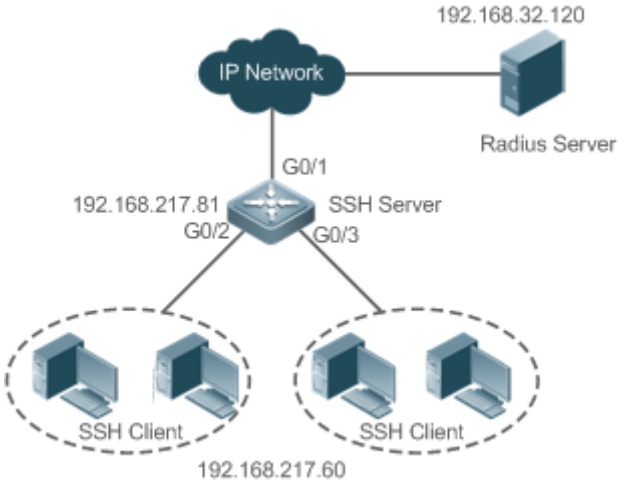


Рисунок 7-17.

Пользователи SSH могут использовать режим аутентификации AAA для аутентификации пользователя, как показано на Рисунке 7-17. Для обеспечения безопасности обмена данными ПК работает как клиент SSH и использует протокол SSH для входа на сетевое устройство, на котором включен сервер SSH. Для более эффективного управления безопасностью в пользовательском интерфейсе входа в систему клиента SSH используется режим аутентификации AAA. Два метода аутентификации, включая аутентификацию сервера Radius и локальную аутентификацию, предусмотрены в списке методов аутентификации AAA для обеспечения надежности. Предпочтительным является метод аутентификации сервера Radius. Если сервер Radius не отвечает, выберите метод локальной аутентификации.

Шаги настройки	• Маршрут от клиента SSH к серверу SSH доступен, и маршрут от сервера SSH к серверу Radius также доступен. • Настройте сервер SSH на сетевом устройстве. Метод настройки уже описан в предыдущем примере и поэтому здесь опущен. • Настройте параметры AAA на сетевом устройстве. Когда используется режим аутентификации AAA, списки методов создаются для определения аутентификации и типов удостоверений и применяются к указанной службе или интерфейсу
SSH-сервер	QTECH(config)# enable service ssh-server QTECH(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok]

	% Generating 512 bit RSA keys ...[ok] QTECH(config)#crypto key generate dsa Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit DSA keys ...[ok] QTECH(config)#interface gigabitEthernet1/1 QTECH(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0 QTECH(config-if-gigabitEthernet1/1)#exit QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#radius-server host 192.168.32.120 QTECH(config)#radius-server key aaaradius QTECH(config)#aaa authentication login methodgroup radius local QTECH(config)#line vty 0 4 QTECH(config-line)#login authentication method QTECH(config-line)#exit QTECH(config)#username user1 privilege 1 password 111 QTECH(config)#username user2 privilege 10 password 222 QTECH(config)#username user3 privilege 15 password 333 QTECH(config)#enable secret w
Проверка	• Запустите команду **show running-config** для отображения текущих конфигураций. • В этом примере предполагается, что используется сервер SAM. • Настройте удаленное SSH-соединение на ПК. • Проверьте пользователя для входа
	QTECH#show run aaa new-model ! aaa authentication login method group radius local ! username user1 password 111 username user2 password 222 username user2 privilege 10 username user3 password 333

```
username user3 privilege 15
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet1/1
no ip proxy-arp
ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
login authentication method
!
End
```

В клиенте SSH выберите **System Management→Device Management** и добавьте IP-адрес устройства **192.168.217.81** и ключ устройства **aaaradius**.

Выберите **Security Management→Device Management Rights** и установите права пользователя для входа в систему.

Выберите **Security Management→Device Administrator** и добавьте имя пользователя **user** и пароль **pass**.

Настройте клиент SSH и настройте соединение с сервером SSH. Подробности смотрите в предыдущем примере.

Введите имя пользователя **user** и пароль **pass**. Убедитесь, что вы можете успешно войти на сервер SSH.

```
QTECH#show users
```

Line	User	Host(s)	Idle	Location
0 con 0	idle	00:00:31		
* 1 vty 0	user	idle	00:00:33	192.168.217.60

Настройка аутентификации с открытым ключом пользователей SSH

Сценарий:



Рисунок 7-18.

Пользователи SSH могут использовать открытый ключ для аутентификации пользователя, а алгоритмом открытого ключа является RSA или DSA, как показано на Рисунке 7-18. SSH настраивается на клиенте таким образом, чтобы между клиентом SSH и сервером SSH устанавливалось безопасное соединение.

Шаги настройки	• Чтобы реализовать аутентификацию с открытым ключом на клиенте, сгенерируйте пару ключей (например, ключ RSA) на клиенте, поместите открытый ключ на SSH-сервер и выберите режим аутентификации с открытым ключом. **ПРИМЕЧАНИЕ:** после создания пары ключей на клиенте необходимо сохранить и загрузить файл открытого ключа на сервер и выполнить настройки, связанные с сервером, прежде чем вы сможете продолжить настройку клиента и соединить клиент с сервером. • После создания ключа на клиенте скопируйте файл открытого ключа с клиента на флэш-память SSH-сервера и свяжите файл с именем пользователя SSH. Пользователь может быть связан с одним открытым ключом RSA и одним открытым ключом DSA
SSH-клиент	Запустите программное обеспечение puttygen.exe на клиенте. Выберите SSH-2 RSA на панели **Parameters** и нажмите **Generate**, чтобы сгенерировать ключ, как показано на Рисунке 7-19.

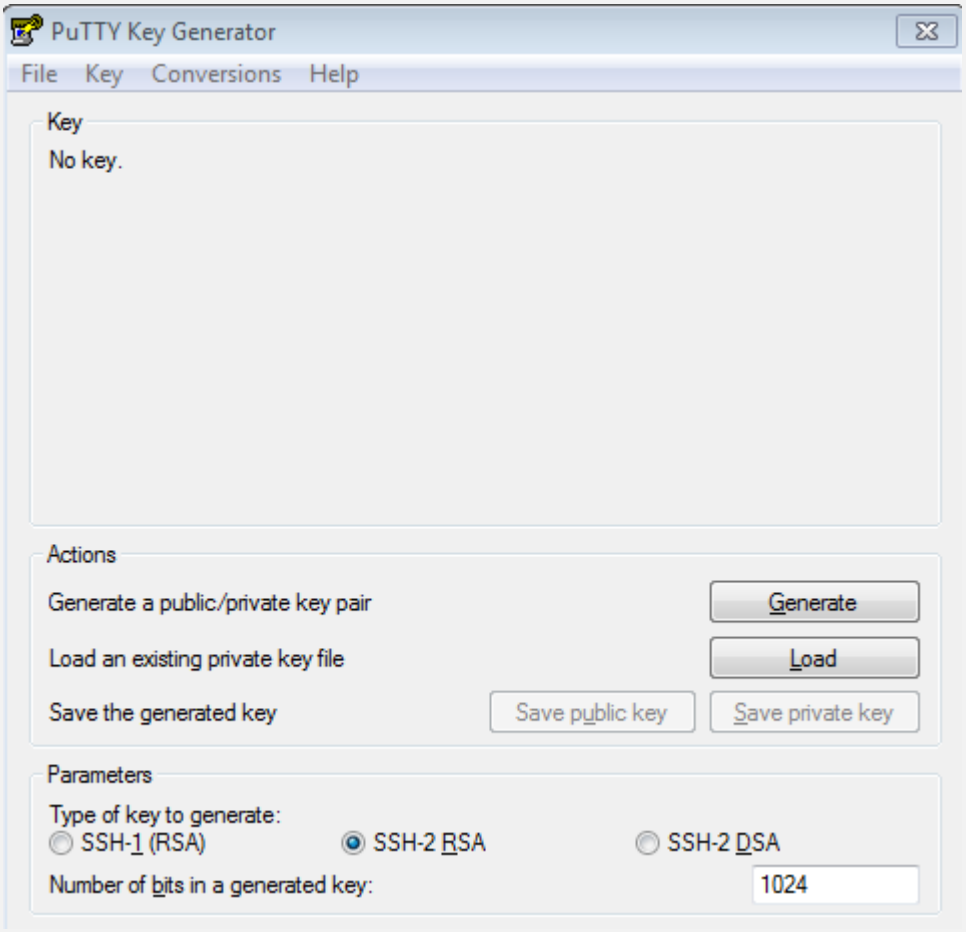


Рисунок 7-19.

Когда ключ генерируется, вам нужно постоянно перемещать мышь по пустой области за пределами зеленого индикатора выполнения; в противном случае индикатор выполнения не перемещается, и генерация ключа останавливается, как показано Рисунке 7-20.

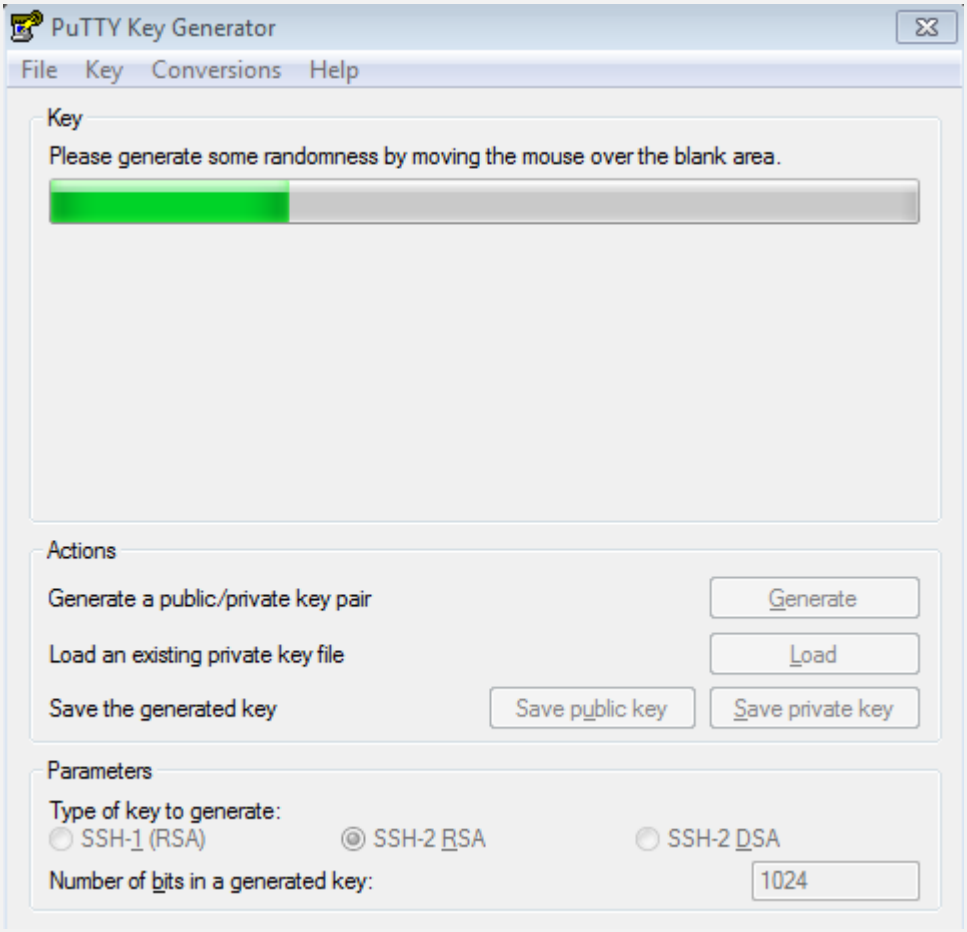


Рисунок 7-20.

Для обеспечения безопасности аутентификации с открытым ключом RSA длина сгенерированной пары ключей RSA должна быть равна или больше 768 бит. В этом примере длина установлена на 1024 бита.

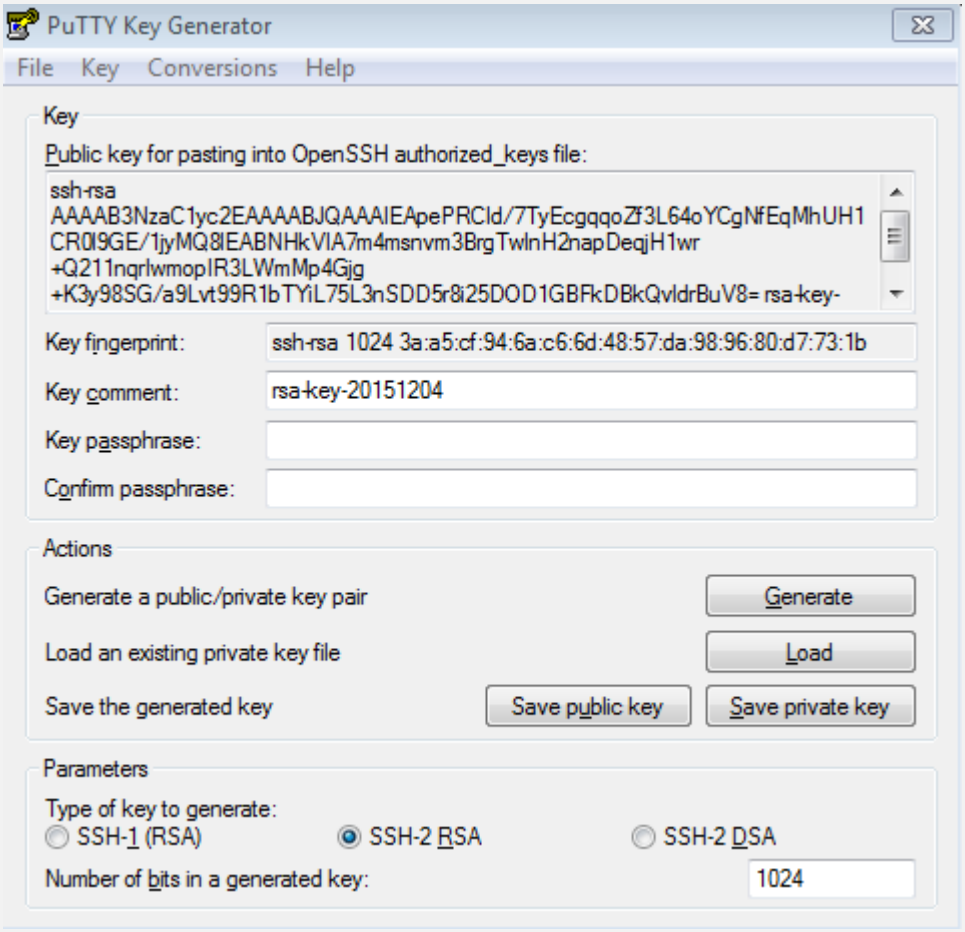


Рисунок 7-21.

После создания пары ключей нажмите **Save public key**, введите имя открытого ключа **test_key.pub**, выберите путь к хранилищу и нажмите **Save**. Затем нажмите **Save private key**. Отображается следующее окно подсказки. Выберите **Yes**, введите имя открытого ключа **test_private** и нажмите **Save**.

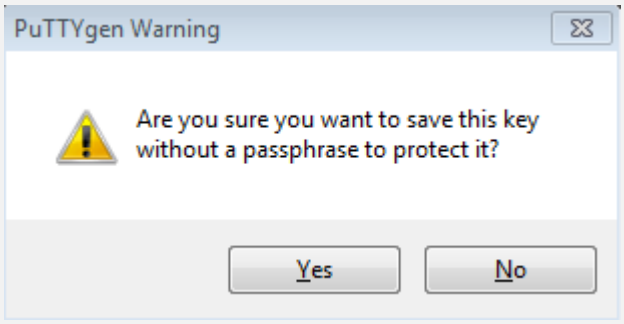
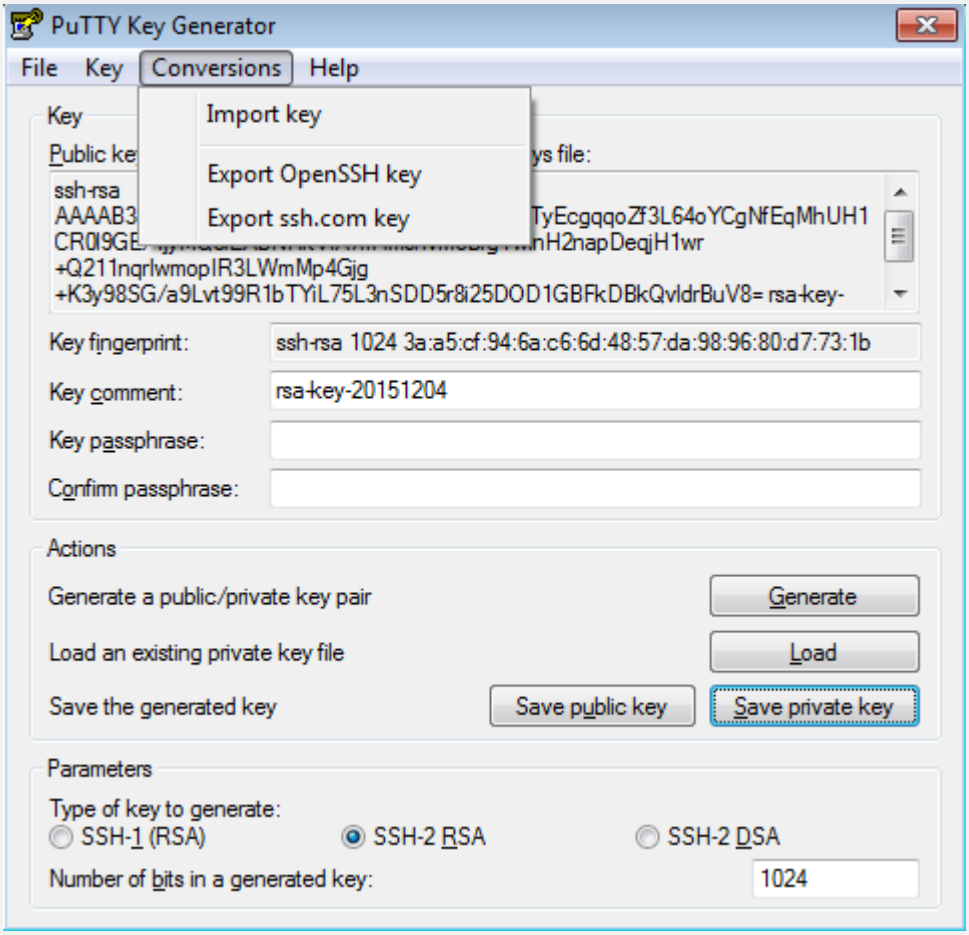


Рисунок 7-22.

Вы должны выбрать файл ключа OpenSSH; в противном случае ключевой файл не может быть использован. Программное обеспечение puttygen.exe можно использовать для создания файла ключа в формате OpenSSH, но клиент PuTTY не может напрямую использовать этот файл. Вы должны использовать puttygen.exe для преобразования закрытого ключа в формат PuTTY. Преобразование формата не требуется для файла открытого ключа,

	хранящегося на сервере, и формат этого файла по-прежнему OpenSSH, как показано на Рисунке 7-23.  Рисунок 7-23
SSH-сервер	QTECH#configure terminal QTECH(config)# ip ssh peer test public-key rsaflash:test_key.pub
Проверка	После завершения основных настроек клиента и сервера укажите файл закрытого ключа **test_private** на клиенте PuTTY и установите IP-адрес хоста на **192.168.23.122** и идентификатор порта на **22**, чтобы установить соединение между клиентом и сервером. Таким образом, клиент может использовать режим аутентификации с открытым ключом для входа в сетевое устройство

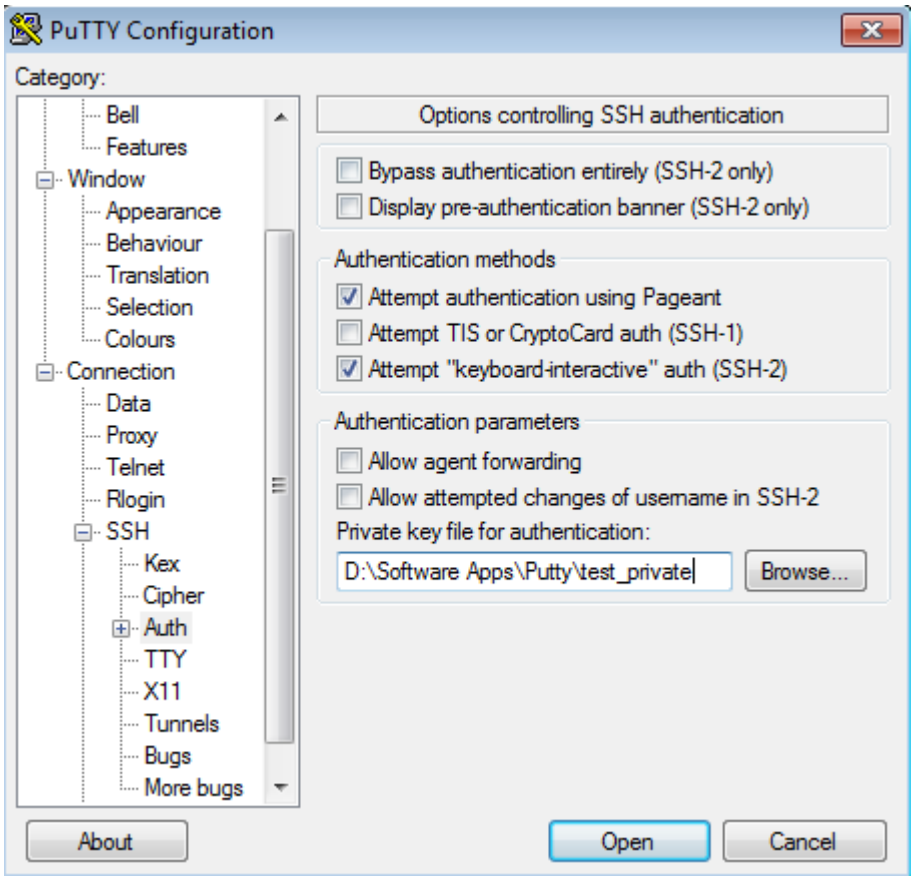


Рисунок 7-24

7.4.1.7. Распространенные ошибки

Команда **no crypto key generate** используется для удаления ключа.

7.4.2. Настройка службы SCP

7.4.2.1. Эффект конфигурации

После включения функции SCP на сетевом устройстве вы можете напрямую загружать файлы с сетевого устройства и загружать локальные файлы на сетевое устройство. Кроме того, все интерактивные данные зашифрованы, что обеспечивает аутентификацию и безопасность.

7.4.2.2. Примечания

Сервер SSH должен быть включен заранее.

7.4.2.3. Шаги настройки

Включение сервера SCP

- Обязательный.
- По умолчанию функция сервера SCP отключена. Запустите команду **ip scp server enable**, чтобы включить функцию сервера SCP в режиме глобальной конфигурации.

7.4.2.4. Проверка

Запустите команду **show ip ssh**, чтобы проверить, включена ли функция сервера SCP.

7.4.2.5. Связанные команды

Включение сервера SCP

Команда	**ip scp server enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для включения сервера SCP. Запустите команду **no ip scp server enable**, чтобы отключить сервер SCP

7.4.2.6. Пример конфигурации

Включение сервера SCP

Шаги настройки	Запустите команду **ip scp server enable**, чтобы включить сервер SCP
	QTECH#configure terminal QTECH(config)#ip scp server enable
Проверка	Запустите команду **show ip ssh**, чтобы проверить, включена ли функция сервера SCP
	QTECH(config)#show ipssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled

Настройка передачи файлов SSH

Сценарий:



Рисунок 7-25.

Служба SCP включена на сервере, а команды SCP используются на клиенте для передачи данных на сервер.

Шаги настройки	• Включите службу SCP на сервере. **ПРИМЕЧАНИЕ:** сервер SCP использует потоки SSH. При подключении к сетевому устройству для передачи SCP клиент занимает сеанс VTY (вы можете узнать, что тип пользователя SSH, выполнив команду **show user**). • На клиенте используйте команды SCP для загрузки файлов на сервер или загрузки файлов с сервера. Syntax of the SCP command: scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-iidentity_file] [-l limit] [-o ssh_option] [-P port] [-S program] [[user@]host1:]file1 [...] [[user@]host2:]file2 Descriptions of some options: -1: Uses SSHv1 (If not specified, SSHv2 is used by default); -2: Uses SSHv2 (by default); -C: Uses compressed transmission. -c: Specifies the encryption algorithm to be used. -r:Transmits the whole directory; -i: Specifies the key file to be used. -l: Limits the transmission speed (unit: Kbit/s). For other parameters, see the filescp.0.
SSH-сервер	QTECH#configure terminal QTECH(config)# ip scp server enable
Проверка	• Пример передачи файлов в системе Ubuntu 7.10: • Установите имя пользователя клиента **test** и скопируйте файл **config.text** с сетевого устройства с IP-адресом 192.168.195.188 в каталог **/root** на локальном устройстве
	root@dhcpd:~#scp test@192.168.23.122:/config.text /root/config.text test@192.168.195.188's password: config.text 100% 1506 1.5KB/s 00:00 Read from remote host 192.168.195.188: Connection reset by peer

7.4.3. Настройка SSH-клиента

7.4.3.1. Эффект конфигурации

На сетевом устройстве, поддерживающем SSH-сервер, включите функцию SSH-сервера и укажите метод аутентификации пользователя и поддерживаемые версии SSH. Затем вы можете использовать встроенную функцию SSH-клиента устройства для установки безопасного соединения с SSH-сервером, реализуя удаленное управление устройством.

7.4.3.2. Примечания

- Функция SSH-сервера должна быть настроена заранее на устройстве, которое должно удаленно поддерживать SSH-сервер.
- Клиент SSH должен правильно взаимодействовать с сервером SSH.

7.4.3.3. Шаги настройки

Указание исходного интерфейса клиента SSH

(Опционально) Эта настройка должна выполняться на клиентском устройстве SSH.

Установление сеанса с сервером SSH

- (Опционально) Используйте команду **ssh** на клиенте, чтобы установить соединение с удаленным сервером.
- Перед использованием этой команды включите функцию сервера SSH и настройте ключ SSH и режим аутентификации на сервере.

Восстановление установленной сессии SSH

(Опционально) Запустите соответствующую команду, чтобы восстановить сеанс после временной остановки, если это необходимо.

Отключение приостановленного сеанса SSH

(Опционально) Эту настройку необходимо выполнить на клиенте SSH, если вам нужно отключить указанный сеанс SSH.

7.4.3.4. Проверка

Запустите команду **show ssh-session**, чтобы отобразить информацию о каждом установленном сеансе клиента SSH.

7.4.3.5. Связанные команды

Указание исходного интерфейса клиента SSH

Команда	**ip ssh source-interface** *interface-name*
Описание параметров	*interface-name*: указывает интерфейс, IP-адрес которого будет использоваться в качестве исходного адреса клиентского сеанса SSH
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для указания интерфейса, IP-адрес которого будет использоваться в качестве глобального исходного адреса сеанса клиента SSH. Когда команда **ssh** используется для подключения к SSH-серверу, эта глобальная конфигурация будет использоваться, если исходный интерфейс или исходный адрес не указаны для этого соединения. Запустите команду **no ip ssh source-interface**, чтобы восстановить настройки по умолчанию

Установление сеанса с сервером SSH

Команда	**ssh [oob] [-v {1 | 2 }][-c {3des | aes128-cbc | aes192-cbc | aes256-cbc }] [-l** *username* **][-m {hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 }] [-p** *port-num*]{ *ip-addr*| *hostname*}[**via** *mgmt-name*][/**source** {**ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name*}] [/**vrf** *vrf-name*]
Описание параметров	**oob**: удаленно подключается к SSH-серверу через внешнюю связь (обычно через интерфейс MGMT). Эта опция доступна, только если устройство имеет интерфейс MGMT. **-v**: (необязательно) указывает версию SSH, используемую для подключения к серверу. SSHv2 используется по умолчанию. **1**: использует SSHv1 для подключения. **2**: использует SSHv2 для подключения. **-c {3des | aes128-cbc | aes192-cbc | aes256-cbc }**: (необязательно) указывает алгоритм шифрования данных, который может быть стандартом шифрования данных (DES), тройным стандартом шифрования данных (3DES) и расширенным стандартом шифрования (AES). Алгоритм AES поддерживает три длины ключа: aes128-cbc (128-битный ключ), aes192-cbc (192-битный ключ) и aes256-cbc (256-битный ключ). • Если **-c** не указан, список всех алгоритмов, поддерживаемых клиентом SSH, отправляется на сервер во время согласования алгоритма. • Если указан параметр **-c**, клиент SSH отправляет на сервер только указанный алгоритм шифрования во время согласования алгоритма. Если сервер не поддерживает указанный алгоритм шифрования, соединение будет отключено. **-l** *username*:(Обязательно) указывает имя пользователя для входа. **-m** {**hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160** }: (Необязательно) указывает алгоритм идентификации хэшированного сообщения (HMAC). • SSHv1 не поддерживает HMAC. Если указаны и SSHv1, и HMAC, HMAC игнорируются. • Если **-m** не указан, список всех алгоритмов, поддерживаемых клиентом SSH, отправляется на сервер во время согласования алгоритма. • Если указан параметр **-m**, клиент SSH отправляет на сервер только указанный алгоритм HMAC во время согласования алгоритма. Если сервер не поддерживает указанный алгоритм HMAC, соединение будет отключено. **-p** *port-num*: (Необязательно) указывает идентификатор порта на клиенте для подключения к удаленному серверу. Идентификатор порта по умолчанию — 22.

	ip-addr| *hostname*: (Обязательный) указывает адрес IPv4/IPv6 или имя хоста удаленного сервера. **via** *mgmt-name*: указывает интерфейс MGMT, используемый при указании **oob**. /**source**: указывает исходный IP-адрес или исходный интерфейс, используемый клиентом SSH. **ip** *A.B.C.D*: указывает исходный IPv4-адрес, используемый клиентом SSH. **ipv6** *X:X:X:X::X*: указывает исходный IPv6-адрес, используемый клиентом SSH. **interface** *interface-name*: указывает исходный интерфейс, используемый клиентом SSH. /**vrf** *vrf-name*: указывает таблицу маршрутизации VRF, используемую для поиска
Командный режим	Пользовательский режим EXEC
Руководство по использованию	Команда **ssh** используется для установки безопасного и зашифрованного соединения локального устройства (клиента SSH) с другим устройством (сервером SSH) или любым другим сервером, поддерживающим SSHv1 или SSHv2. Это соединение обеспечивает механизм, аналогичный соединению Telnet, за исключением того, что все данные, передаваемые по этому соединению, шифруются. На основе аутентификации и шифрования клиент SSH может установить безопасное соединение в небезопасной сети. **ПРИМЕЧАНИЕ:** SSHv1 поддерживает только алгоритмы шифрования DES (56-битный ключ) и 3DES (168-битный ключ). **ПРИМЕЧАНИЕ:** SSHv2 поддерживает следующие расширенные стандарты шифрования (AES): ASE128-CBC, AES192-CBC, AES256-CBC, AES128-CTR, AES192-CTR и AES256-CTR. **ПРИМЕЧАНИЕ:** SSHv1 не поддерживает хешированный код аутентификации сообщений (HMAC). **ПРИМЕЧАНИЕ:** если вы укажете несогласованный алгоритм шифрования или аутентификации при выборе версии SSH, несогласованный алгоритм будет проигнорирован при установке соединения

Восстановление установленного сеанса клиента SSH

Команда	**ssh-session** *session-id*
Описание параметров	*session-id*: указывает идентификатор установленного сеанса клиента SSH

Командный режим	Пользовательский режим EXEC
Руководство по использованию	Эта команда используется для восстановления использования установленного сеанса клиента SSH. Когда команда **ssh** используется для запуска сеанса клиента SSH, вы можете нажать Ctrl+Shift+6+X, чтобы временно выйти из сеанса. Чтобы восстановить этот сеанс, запустите команду **ssh-session**. Кроме того, если сеанс уже установлен, вы можете запустить команду **show ssh-session** для отображения информации об установленном сеансе

Отключение приостановленного сеанса SSH

Команда	**disconnect ssh-session** *session-id*
Описание параметров	*session-id*: указывает идентификатор приостановленного сеанса клиента SSH
Командный режим	Пользовательский режим EXEC
Руководство по использованию	Вы можете указать идентификатор сеанса клиента SSH, чтобы отключить указанный сеанс клиента SSH

7.4.3.6. Пример конфигурации

Указание исходного интерфейса клиента SSH

Шаги настройки	Запустите команду **ip ssh source-interface** *interface-name*, чтобы указать интерфейс, IP-адрес которого будет использоваться в качестве глобального исходного адреса клиентского сеанса SSH
	QTECH#configure terminal QTECH(config)#ipsshsource-interface gigabitEthernet 0/1

Установление сеанса с сервером SSH

Сценарий:



Рисунок 7-26.

На сервере включена функция SSH-сервера. Команда **ssh** используется на клиенте для установки безопасного соединения с сервером.

Шаги настройки	• Включите функцию SSH-сервера на сервере. • Настройте ключ SSH на сервере. • Настройте режим аутентификации сервера SSH и используйте режим аутентификации локальной учетной записи для чтрок 0–4. • Настройте IP-адрес интерфейса Gi 0/1 сервера SSH. Клиент будет использовать этот адрес в качестве исходного адреса для подключения к SSH-серверу. • Настройте клиент SSH и укажите исходный адрес клиента SSH. **ПРИМЕЧАНИЕ:** по умолчанию сервер SSH поддерживает две версии SSH: SSHv1 и SSHv2. **ПРИМЕЧАНИЕ:** с помощью этого ключа SSH-сервер расшифровывает зашифрованный пароль, полученный от SSH-клиента, сравнивает расшифрованный открытый текст с паролем, хранящимся на сервере, и возвращает сообщение об успешной или неудачной аутентификации. SSHv1 использует ключ RSA, тогда как SSHv2 использует ключ RSA или DSA. **ПРИМЕЧАНИЕ:** режим аутентификации, используемый сервером SSH, — аутентификация по локальной учетной записи. Локальное имя пользователя — admin, пароль — 123456. **ПРИМЕЧАНИЕ:** клиент SSH подключается к серверу SSH на основе этого IP-адреса. Маршруты от клиентов SSH к серверу SSH доступны. **ПРИМЕЧАНИЕ:** настройте IP-адрес интерфейса Gi 0/1 сервера SSH. Клиент будет использовать этот адрес в качестве исходного адреса для подключения к SSH-серверу
SSH-сервер	QTECH#configure terminal QTECH(config)#enable service ssh-server QTECH(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] QTECH(config)#line vty 0 4 QTECH(config-line)#login local QTECH(config-line)#exit QTECH(config)#username admin password 123456 QTECH(config)#username admin privilege 15

	QTECH(config-line)#exit QTECH(config)#interface gigabitEthernet0/1 QTECH(config-if-gigabitEthernet0/1)#ip address 192.168.23.122 255.255.255.0 QTECH(config-if-gigabitEthernet0/1)#exit
SSH-клиент	QTECH(config)#interface gigabitEthernet0/1 QTECH(config-if-gigabitEthernet0/1)#ip address 192.168.23.83 255.255.255.0 QTECH(config-if-gigabitEthernet0/1)#exit QTECH(config)#ipsshsource-interface gigabitEthernet 0/1
Проверка	• Запустите команды **show running-config| include username** и **show ip ssh**, чтобы проверить правильность конфигурации сервера SSH. • На клиенте SSH настройте соединение с удаленным сервером SSH. После установки соединения введите правильный пароль **123456**. Отобразится интерфейс работы SSH-сервера. Проверьте учетную запись пользователя для входа в консоль клиента SSH
	QTECH(config)#sh running-config | include username username admin password admin username admin privilege 15 QTECH(config)#sh running-config | begin line line con 0 line vty 0 4 login local ! ! end
	Проверьте правильность конфигурации клиента SSH
	QTECH#ssh -l admin 192.168.23.122 %Trying 192.168.23.122, 22,...open admin@192.168.23.122's password: QTECH# QTECH#sh users Line User Host(s) Idle Location 0 con 0 idle 00:00:00 * 1 vty 0 admin idle 00:00:36 192.168.217.20

7.4.4. Настройка SCP-клиента

7.4.4.1. Эффект конфигурации

На сетевом устройстве, поддерживающем сервер SCP, включите службу SCP, чтобы пользователи могли напрямую загружать файлы с сетевого устройства и загружать локальные файлы на сетевое устройство. Кроме того, все обмениваемые данные шифруются, обеспечивая аутентификацию и безопасность.

7.4.4.2. Примечания

- Функция сервера SSH должна быть настроена, а служба SCP должна быть включена на устройстве для удаленной поддержки сервера SCP.
- Клиент SCP должен правильно взаимодействовать с сервером SCP.

7.4.4.3. Шаги настройки

Указание исходного интерфейса клиента SCP

(Необязательно) Укажите исходный интерфейс клиента SCP.

Реализация передачи файлов с SCP-сервером через SCP-клиент

- (Необязательно) Запустите команду **scp**, чтобы реализовать передачу файлов на удаленный сервер SCP через клиент SCP.
- Перед выполнением этой команды включите функцию сервера SSH, настройте ключ SSH и режим аутентификации, а также включите функцию сервера SCP.

7.4.4.4. Проверка

Проверьте, прошла ли передача файла успешно.

7.4.4.5. Связанные команды

Указание исходного интерфейса клиента SCP

Команда	**ip scp client source-interface** *interface-name*
Описание параметров	*interface-name*: указывает исходный интерфейс. Установите IP-адрес интерфейса на исходный IP-адрес SCP-клиента
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы указать IP-адрес назначенного интерфейса в качестве глобального исходного адреса клиента SCP. При взаимодействии с удаленным SSH-сервером через команду **scp** используются глобальные настройки, если не указан исходный интерфейс или исходный адрес. Запустите команду **no ip ssh source-interface** для восстановления настроек по умолчанию

Реализация передачи файлов с SCP-сервером через SCP-клиент

Команда	**scp [oob] [-v { 1 | 2 }] [-c { 3des | aes128-cbc | aes192-cbc | aes256-cbc }] [-m { hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 }] [-p** *port-num*] { **filename username@host:/filename | username@host:/filename filename} [via** *mgmt-name*] [**/source { ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* }] [**/vrf** *vrf-name*]
Описание параметров	**oob**: удаленно подключается к серверу SCP через внешнюю связь (обычно через интерфейс MGMT). Эта опция доступна, только если устройство имеет интерфейс MGMT. **-v**: (необязательно) указывает версию SSH, используемую для подключения к серверу. SSHv2 используется по умолчанию. **1**: использует SSHv1 для подключения. **2**: использует SSHv2 для подключения. **-c { 3des | aes128-cbc | aes192-cbc | aes256-cbc }**: (необязательно) указывает алгоритм шифрования данных, который может быть стандартом шифрования данных (DES), тройным стандартом шифрования данных (3DES) и расширенным стандартом шифрования (AES). Алгоритм AES поддерживает три длины ключа: aes128-cbc (128-битный ключ), aes192-cbc (192-битный ключ) и aes256-cbc (256-битный ключ). • Если **-c** не указан, список всех алгоритмов, поддерживаемых клиентом SSH, отправляется на сервер во время согласования алгоритма. • Если указан параметр **-c**, клиент SSH отправляет на сервер только указанный алгоритм шифрования во время согласования алгоритма. Если сервер не поддерживает указанный алгоритм шифрования, соединение будет отключено. **-m { hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 }**: (Необязательно) указывает алгоритм идентификации хэшированного сообщения (HMAC). • SSHv1 не поддерживает HMAC. Если указаны и SSHv1, и HMAC, HMAC игнорируются. • Если **-m** не указан, список всех алгоритмов, поддерживаемых клиентом SCP, отправляется на сервер во время согласования алгоритма. • Если указан параметр **-m**, клиент SCP отправляет на сервер только указанный алгоритм HMAC во время согласования алгоритма. Если сервер не поддерживает указанный алгоритм HMAC, соединение будет отключено. **-p** *port-num*: (Необязательно) указывает идентификатор порта на клиенте для подключения к удаленному серверу. Идентификатор порта по умолчанию — **22**. **filename username@host:/filename | username@host:/filename filename**: (Обязательно) filename username@host:/filename указывает на загрузку файла с устройства на удаленный сервер SCP.

	username@host:/filename filename указывает на загрузку файла с удаленного сервера SCP на устройство. Файлы на устройстве поддерживают следующие носители: flash:/filename: extended flash memory flash2:/filename: extended flash memory 2 usb0:/filename: extended USB flash drive 0. Поддерживается только в том случае, если устройство имеет один USB-порт и вставлен расширенный USB-накопитель. usb1:/filename: extended USB flash drive 1. Поддерживается только в том случае, если устройство имеет два USB-порта и вставлены расширенные USB-накопители. sd0:/filename: extended SD card. Поддерживается только в том случае, если на устройстве есть один порт SD-карты и вставлена расширенная SD-карта. sata0:/filename: extended hard disk device. tmp:/filename: temporary directory **tmp/vsd/.** *ip-addr* | *hostname*: (Обязательный) указывает адрес IPv4/IPv6 или имя хоста удаленного сервера. **via** *mgmt-name*: указывает интерфейс MGMT, используемый при указании **oob**. **/source**: указывает исходный IP-адрес или исходный интерфейс, используемый клиентом SCP. **ip** *A.B.C.D*: указывает исходный адрес IPv4, используемый клиентом SCP. **ipv6** *X:X:X:X::X*: указывает исходный IPv6-адрес, используемый клиентом SCP. **interface** *interface-name*: указывает исходный интерфейс, используемый клиентом SCP. **/vrf** *vrf-name*: указывает таблицу маршрутизации VRF, используемую для поиска
Командный режим	Общий пользовательский режим
Руководство по использованию	Запустите команду **scp** для установки безопасного и зашифрованного соединения с локального устройства (клиент SCP) на другое устройство (сервер SCP) для реализации передачи файлов

7.4.4.6. Пример конфигурации

Указание исходного интерфейса клиента SCP

Шаги настройки	Запустите команду **ip scp client source-interface** *interface-name*, чтобы указать IP-адрес интерфейса в качестве глобального исходного адреса клиента SCP

	QTECH# configure terminal QTECH(config)# ip scp client source-interface gigabitEthernet 0/1

Реализация передачи файлов с SCP-сервером через SCP-клиент

Сценарий:



Рисунок 7-27.

Включите функции SSH-сервера и SCP-сервера на стороне сервера и запустите команду **scp** на клиенте SCP для реализации передачи файлов с сервером.

Шаги настройки	• Включите функцию сервера SSH на стороне сервера. • Настройте ключ SSH на стороне сервера. • Настройте режим аутентификации для сервера SSH и настройте режим локальной аутентификации для строк с 0 по 4. • Включите функцию сервера SCP. • Настройте IP-адрес интерфейса Gi 0/1 сервера SSH, чтобы клиент использовал этот адрес в качестве исходного адреса для подключения к серверу SSH. • Настройте клиент SSH и укажите исходный адрес клиента SSH. **ПРИМЕЧАНИЕ:** по умолчанию сервер SSH поддерживает две версии SSH: SSHv1 и SSHv2. **ПРИМЕЧАНИЕ:** с помощью этого ключа сервер SSH расшифровывает зашифрованный пароль, полученный от клиента SSH, сравнивает расшифрованный простой текст с паролем, хранящимся на сервере, и возвращает сообщение об успешной или неудачной аутентификации. SSHv1 использует ключ RSA, а SSHv2 использует ключ RSA или DSA. **ПРИМЕЧАНИЕ:** сервер SSH использует локальный режим аутентификации. Локальное имя пользователя — **admin**, а пароль **123456**. **ПРИМЕЧАНИЕ:** клиент SSH подключается к серверу SSH по этому IP-адресу. Маршрут от клиента SSH к серверу SSH доступен. **ПРИМЕЧАНИЕ:** настройте IP-адрес интерфейса Gi 0/1 клиента SSH, чтобы клиент использовал этот адрес в качестве исходного адреса для подключения к серверу SSH
SCP-сервер	QTECH# configure terminal QTECH(config)#enable service ssh-server QTECH(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]:

	Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] QTECH(config)#line vty 0 4 QTECH(config-line)#login local QTECH(config-line)#exit QTECH(config)#username admin password 123456 QTECH(config)#username admin privilege 15 QTECH(config-line)#exit QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.23.122 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit
SSH-клиент	QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.23.83 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit QTECH(config)# ip scp server enable QTECH(config)#ip ssh source-interface gigabitEthernet 0/1
Проверка	• Запустите команды **show running-config | include username** и **show ip ssh** для проверки конфигурации SSH-сервера. • На клиенте SSH настройте соединение с удаленным SSH-сервером. После того, как соединение установлено, введите пароль 123456. Отобразится интерфейс работы SSH-сервера. Проверьте вошедшего в систему пользователя на консоли клиента SSH
	QTECH(config)#sh running-config | include username username admin password admin username admin privilege 15 QTECH(config)#sh running-config | begin line line con 0 line vty 0 4 login local ! ! end

	Проверьте конфигурацию клиента SCP
	QTECH#scp config.text admin@192.168.23.122:/config.text %Trying 192.168.23.122, 22,...open admin@192.168.23.122's password: QTECH#

7.5. Мониторинг

7.5.1. Отображение

Описание	Команда
Отображает действующие конфигурации SSH-сервера	**show ipssh**
Отображает установленное соединение SSH	**show ssh**
Отображает общедоступную информацию об открытом ключе SSH	**show crypto key mypubkey**
Отображает установленный сеанс клиента SSH	**show ssh-session**

7.5.2. Отладка

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

Описание	Команда
Отладка сеансов SSH	**debug ssh**
Отладка клиентских сеансов SSH	**debug ssh client**

8. НАСТРОЙКА URPF

8.1. Обзор

Одноадресная переадресация по обратному пути (URPF) — это функция, защищающая сеть от подделки исходного адреса.

URPF получает исходный адрес и входящий интерфейс полученного пакета и ищет запись о пересылке в таблице переадресации на основе исходного адреса. Если запись не существует, пакет отбрасывается. Если исходящий интерфейс записи пересылки не соответствует входящему интерфейсу пакета, пакет также отбрасывается. В противном случае пакет пересылается.

URPF реализован в двух режимах:

- Строгий режим: он часто развертывается на интерфейсе точка-точка (P2P), а входящие и исходящие потоки данных должны проходить через сеть интерфейса P2P.
- Свободный режим: он применим к асимметричным маршрутам или многосетевым сетям, в которых существует проблема асимметричного трафика.

8.1.1. Протоколы и стандарты

- RFC 2827: фильтрация сетевых входов: DDOS-атаки, использующие спуфинг (подмену) IP-адреса источника
- RFC 3704: фильтрация входящего трафика для многосетевых сетей

8.2. Приложения

Приложение	Описание
Строгий режим	Блокирует пакеты с поддельными исходными адресами на уровне доступа или уровне агрегации, чтобы предотвратить отправку этих пакетов с ПК в базовую сеть
Свободный режим	В многосетевой сети пользовательская сеть подключена к нескольким поставщикам услуг Интернета (ISP), а входящий и исходящий трафик несимметричны. Разверните свободный режим URPF на исходящем интерфейсе, подключенном к интернет-провайдерам, чтобы предотвратить атаку недопустимых пакетов на пользовательскую сеть

8.2.1. Строгий режим

8.2.1.1. Сценарий

Злоумышленник инициирует атаку, отправляя пакеты с поддельным адресом источника 11.0.0.1. В результате сервер отправляет много пакетов SYN или ACK на хосты, которые не инициируют атаку, а также хост с реальным адресом источника 11.0.0.1. Даже хуже, если сетевой администратор определяет, что этот адрес инициирует атаку на сеть, и поэтому блокирует все потоки данных, идущие с этого исходного адреса, происходит отказ в обслуживании (DoS) этого исходного адреса.

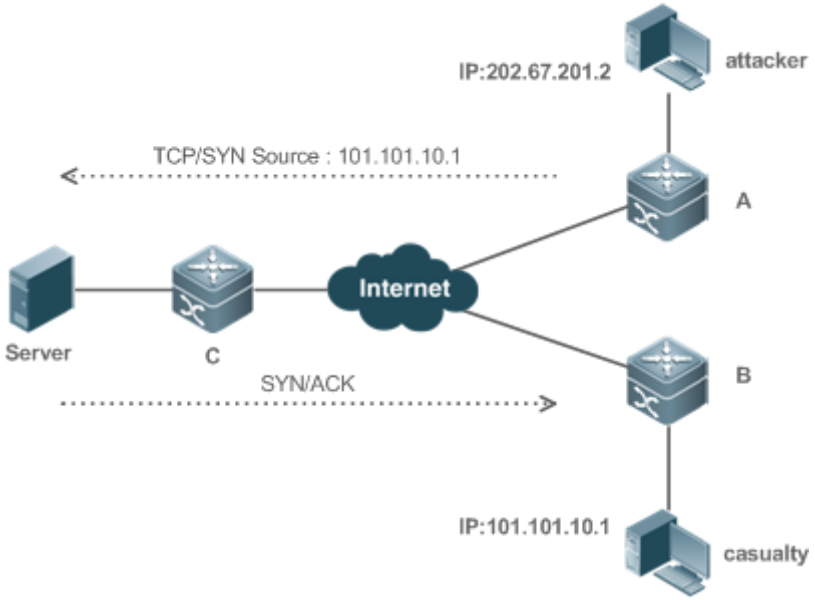


Рисунок 8-1.

Злоумышленник отправляет поддельные пакеты, используя поддельный адрес пострадавшего.

8.2.1.2. Развертывание

Разверните строгий режим URPF на устройстве A, чтобы защитить устройство от спуфинга исходного адреса.

8.2.2. Свободный режим

8.2.2.1. Сценарий

Асимметричный маршрут — это распространенное сетевое приложение, используемое для управления сетевым трафиком или для выполнения требований политики маршрутизации.

Как показано на Рисунке 8-2, если на интерфейсе G1/1 маршрутизатора R1 включен строгий режим URPF, R1 получает пакет из сегмента сети 192.168.20.0/24 на интерфейсе G1/1, но полученный через проверку URPF интерфейс — G1/2. Поэтому этот пакет не проходит проверку URPF и отбрасывается.

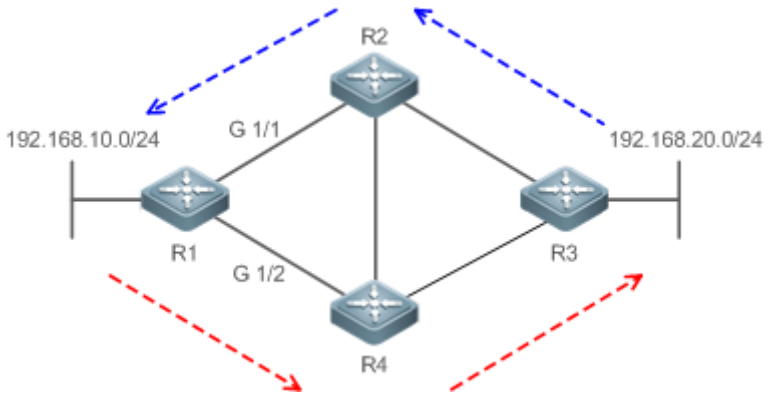


Рисунок 8-2.

8.2.2.2. Развертывание

- Обратный поиск маршрута на основе исходного IP-адреса полученного пакета. Цель состоит в том, чтобы найти маршрут, и не требуется, чтобы исходящий интерфейс next hop'a на маршруте был входящим интерфейсом полученного пакета.
- Свободный режим URPF может решить проблему асимметричного трафика асимметричного маршрута и предотвратить доступ к недопустимым потокам данных.

8.3. Функции

8.3.1. Базовые концепты

Строгий режим URPF

Получите исходный адрес и входящий интерфейс полученного пакета и найдите запись о пересылке в таблице переадресации на основе исходного адреса. Если запись не существует, пакет отбрасывается. Если исходящий интерфейс записи пересылки не соответствует входящему интерфейсу пакета, пакет также отбрасывается. Строгий режим требует, чтобы входящий интерфейс полученного пакета был исходящим интерфейсом записи маршрута к исходному адресу пакета.

Свободный режим URPF

Обратный поиск маршрута на основе исходного IP-адреса полученного пакета. Цель состоит в том, чтобы найти маршрут, и не требуется, чтобы исходящий интерфейс next hop'a на маршруте был входящим интерфейсом полученного пакета. Однако маршрут не может быть маршрутом хоста в локальной сети.

Скорость потери пакетов URPF

Скорость потери пакетов URPF равна количеству пакетов, отброшенных из-за проверки URPF в секунду. Единица измерения — пакеты в секунду, то есть пак/с (pps).

Интервал расчета коэффициента потери пакетов URPF

Это интервал от предыдущего момента расчета коэффициента потери пакетов до текущего момента расчета коэффициента потери пакетов.

Интервал выборки скорости потери пакетов URPF

Это интервал, с которым собирается количество потерянных пакетов для расчета коэффициента потери пакетов. Этот интервал должен быть больше или равен интервалу расчета коэффициента потери пакетов.

Порог скорости потери пакетов URPF

Это относится к максимальной скорости потери пакетов, которая является приемлемой. Когда скорость потери пакетов превышает пороговое значение, пользователям могут отправляться аварийные сигналы через системные журналы или сообщения trap. Вы можете настроить порог скорости потери пакетов в зависимости от реальных условий сети.

Интервал оповещений скорости потери пакетов URPF

Это интервал, с которым оповещения отправляются пользователям. Вы можете настроить сигнал оповещений в зависимости от фактических условий сети, чтобы предотвратить частый вывод журналов или сообщений trap.

Расчет коэффициента потери пакетов URPS

Между периодом времени от включения URPF до времени, когда приходит интервал выборки, коэффициент потери пакетов равен количеству потерянных пакетов,

измеренному в интервале выборки, деленному на продолжительность включения URPF. После этого скорость потери пакетов рассчитывается следующим образом: Текущая скорость потери пакетов = (Текущее количество потерянных пакетов, измеренное в интервале расчета – Количество потерянных пакетов, измеренное до интервала выборки)/Интервал выборки.

8.3.2. Обзор

Особенность	Описание
Включение URPF	Включите URPF для выполнения проверки URPF, тем самым защитив устройство от спуфинга исходного адреса
Уведомление о коэффициенте потери пакетов URPF	Чтобы упростить мониторинг информации о потерянных пакетах после включения URPF, устройства QTECH поддерживают использование системных журналов и сообщений trap для упреждающего уведомления пользователей об информации о потере пакетов, обнаруженной при проверке URPF

8.3.3. Включение URPF

Включите URPF для выполнения проверки URPF для IP-пакетов, тем самым защитив устройство от подмены (спуфинга) исходного адреса.

8.3.3.1. Принцип работы

URPF может применяться к IP-пакетам на основе конфигураций, но следующие пакеты не проверяются URPF:

1. После включения URPF исходный адрес пакета проверяется только в том случае, если адрес назначения пакета является unicast-адресом IPv4/IPv6, и не проверяется, если пакет является многоадресным или широковещательным IP-пакетом.
2. Если IP-адрес источника пакета DHCP/BOOTP равен 0.0.0.0, а IP-адрес получателя — 255.255.255.255, пакет не проверяется URPF.
3. Пакет loopback, отправленный локальным устройством самому себе, не проверяется URPF.

URPF, настроенная в режиме конфигурации интерфейса

URPF выполняется для пакетов, полученных на сконфигурированном интерфейсе. Конфигурации в режиме конфигурации интерфейса и в режиме глобальной конфигурации не могут сосуществовать.

- По умолчанию маршрут по умолчанию не используется для проверки URPF. При необходимости вы можете настроить данные для использования маршрута по умолчанию для проверки URPF.
- По умолчанию пакеты, не прошедшие проверку URPF, будут отброшены. Если ACL (*acl-name*) настроен, пакет сопоставляется с ACL после того, как он терпит неудачу в проверке URPF. Если ACL не существует или пакет соответствует записи отказа в ACL (deny ACE), пакет будет отброшен. Если пакет соответствует permit ACE (разрешение), пакет будет перенаправлен.

ПРИМЕЧАНИЕ: коммутатор поддерживает настройку URPF на маршрутизируемом порту агрегированного порта L3 (AP). В некоторых случаях конфигурация также поддерживается на SVI. Существуют следующие ограничения:

- URPF не поддерживает ассоциацию с параметром ACL.
- После включения URPF на интерфейсах выполняется проверка URPF для всех пакетов, полученных на физические порты, соответствующие этим интерфейсам, что увеличивает объем пакетов, проверяемых URPF. Если пакет, полученный на туннельном порту, также получен на предыдущих физических портах, пакет также проверяется URPF. В таком случае будьте осторожны при включении URPF.
- После включения URPF пропускная способность пересылки маршрута устройства будет уменьшена наполовину.
- После включения строгого режима URPF, если пакет, полученный на интерфейсе, совпадает с маршрутом «равной стоимости» во время проверки URPF, пакет будет обработан в соответствии со свободным режимом URPF.

8.3.3.2. Связанная конфигурация

Включение URPF для указанного интерфейса

По умолчанию URPF отключен для указанного интерфейса.

Запустите команду **ip verify unicast source reachable-via** {**rx** | **any** }[**allow-default**][*acl-name*] для включения или отключения функции IPv4 URPF для указанного интерфейса.

По умолчанию маршрут по умолчанию не используется для проверки URPF. Вы можете использовать ключевое слово **allow-default**, чтобы использовать маршрут по умолчанию для проверки URPF, если это необходимо.

По умолчанию пакеты, не прошедшие проверку URPF, будут отброшены. Если ACL (*acl-name*) настроен, пакет сопоставляется с ACL после того, как он терпит неудачу в проверке URPF. Если ACL не существует или пакет соответствует deny ACE (отказ), пакет будет отброшен. Если пакет соответствует permit ACE (разрешение), пакет будет перенаправлен.

8.3.4. Уведомление о коэффициенте потери пакетов URPF

Чтобы упростить мониторинг информации о потерянных пакетах после включения URPF, устройства QTECH поддерживают использование системных журналов и сообщений trap для упреждающего уведомления пользователей об информации о потере пакетов, обнаруженной при проверке URPF.

8.3.4.1. Принцип работы

Между периодом времени от включения URPF до времени, когда приходит интервал выборки, коэффициент потери пакетов равен количеству потерянных пакетов, измеренному в интервале выборки, деленному на продолжительность включения URPF. После этого скорость потери пакетов рассчитывается следующим образом: Текущая скорость потери пакетов = (Текущее количество потерянных пакетов, измеренное в интервале расчета – Количество потерянных пакетов, измеренное до интервала выборки)/Интервал выборки.

После включения функции мониторинга информации о потере пакетов URPF устройство может заранее отправлять системные журналы или сообщения trap, чтобы уведомить пользователей об информации о потере пакетов, обнаруженной при проверке URPF, чтобы пользователи могли удобно отслеживать состояние сети.

8.3.4.2. Связанная конфигурация

Настройка интервала расчета скорости потери пакетов URPF

По умолчанию интервал расчета скорости потери пакетов URPF составляет 30 секунд. Если интервал расчета слишком короткий, запустите команду **ip verify urpf drop-rate compute interval** *seconds*, чтобы изменить интервал расчета.

Интервал расчета скорости потери пакетов URPF составляет от 30 до 300.

Настройка интервала оповещения скорости потери пакетов URPF

По умолчанию интервал оповещения скорости потери пакетов URPF составляет 300 секунд. Если интервал оповещений окажется неподходящим, запустите команду **ip verify urpf drop-rate notify hold-down** *seconds*, чтобы изменить интервал оповещений скорости потери пакетов URPF.

Единицей интервала оповещений является секунда. Значение колеблется от 30 до 300.

Настройка функции мониторинга информации о потере пакетов URPF

По умолчанию функция мониторинга информации о потере пакетов URPF отключена.

Запустите команду **ip** [**ipv6**] **verify urpf drop-rate notify**, чтобы включить или отключить функцию мониторинга информации о потере пакетов URPF.

Настройка порога скорости потери пакетов URPF

По умолчанию порог скорости потери пакетов URPF составляет 1000 пакетов в секунду. Если порог не подходит, запустите команду **ip [ipv6] verify urpf notification threshold** *rate-value*, чтобы изменить порог скорости потери пакетов URPF.

Единицей порога является пак/с. Значение находится в диапазоне от 0 до 4 294 967 295.

8.4. Конфигурация

8.4.1. Включение URPF

8.4.1.1. Эффект конфигурации

- Включите URPF для выполнения проверки URPF для IP-пакетов, тем самым защитив устройство от подмены (спуфинга) исходного адреса.
- URPF, включенный в режиме конфигурации интерфейса, поддерживает как строгий, так и свободный режимы.

8.4.1.2. Примечания

URPF реализуется с помощью существующих в сети одноадресных маршрутов. Поэтому в сети должны быть настроены одноадресные маршруты.

8.4.1.3. Шаги настройки

Включение IPv4 URPF для указанного интерфейса

Обязательный.

8.4.1.4. Проверка

Включите URPF и проверьте исходный адрес следующим образом:

- Если используется строгий режим, проверяйте, пересылается ли пакет, только когда таблица пересылки содержит исходный адрес полученного IP-пакета, а исходящий интерфейс искомой записи пересылки совпадает с входящим интерфейсом пакета; в противном случае пакет отбрасывается.

- Если используется свободный режим, проверьте, переадресовывается ли пакет, когда в таблице переадресации можно найти запись о пересылке для исходного адреса полученного IP-пакета; в противном случае пакет отбрасывается.

8.4.1.5. Связанные команды

Включение IPv4 URPF для указанного интерфейса

Команда	**ip verify unicast source reachable-via { any | rx } [allow-default]** [acl-number]
Описание параметров	**rx**: указывает, что проверка URPF реализована в строгом режиме. Строгий режим требует, чтобы исходящий интерфейс записи пересылки, найденной в таблице переадресации на основе исходного адреса полученного IP-пакета, совпадал с входящим интерфейсом пакета. **any**: указывает, что проверка URPF выполняется в свободном режиме. Свободный режим требует только того, чтобы в таблице переадресации можно было найти запись о переадресации на основе исходного адреса полученного IP-пакета. **allow-default**: (Необязательно) указывает, что для проверки URPF можно использовать маршрут по умолчанию. *acl-id*: (Необязательно) указывает идентификатор ACL. Значения включают от 1 до 99 (стандартный список доступа IP), от 100 до 199 (расширенный список доступа IP), от 1300 до 1999 (стандартный список доступа IP, расширенный диапазон) и от 2000 до 2699 (расширенный список доступа IP, расширенный диапазон)
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	На основе исходного адреса полученного IP-пакета URPF проверяет, существует ли какой-либо маршрут к исходному адресу в таблице переадресации, и соответственно определяет, является ли пакет действительным. Если ни одна запись переадресации не соответствует, пакет определяется как недействительный. Вы можете включить URPF в режиме конфигурации интерфейса, чтобы выполнять проверку URPF для пакетов, полученных на интерфейсе. По умолчанию маршрут по умолчанию не используется для проверки URPF. Вы можете использовать ключевое слово **allow-default**, чтобы использовать маршрут по умолчанию для проверки URPF, если это необходимо. По умолчанию пакеты, не прошедшие проверку URPF, будут отброшены. Если ACL (*acl-name*) настроен, пакет сопоставляется с ACL после того, как он терпит неудачу в проверке URPF. Если ACL не существует или пакет соответствует deny ACE (отказ), пакет будет отброшен. Если пакет соответствует permit ACE (разрешение), пакет будет перенаправлен.

	ПРИМЕЧАНИЕ: коммутатор поддерживает настройку URPF на маршрутизируемом порту или агрегируемом порту L3. Кроме того, существуют следующие ограничения: 1. URPF не поддерживает ассоциацию с параметром ACL. 2. После включения URPF на интерфейсах выполняется проверка URPF для всех пакетов, полученных на физические порты, соответствующие этим интерфейсам, что увеличивает объем пакетов, проверяемых URPF. Если пакет, полученный на туннельном порту, также получен на предыдущих физических портах, пакет также проверяется URPF. В таком случае будьте осторожны при включении URPF. 3. После включения URPF пропускная способность переадресации маршрута устройства будет уменьшена наполовину. 4. После включения строгого режима URPF, если пакет, полученный на интерфейсе, совпадает с маршрутом «равной стоимости» во время проверки URPF, пакет будет обработан в соответствии со свободным режимом URPF. 5. Если URPF настроен в режиме глобальной конфигурации, маршрут по умолчанию нельзя использовать для проверки URPF.

8.5. Мониторинг

8.5.1. Очистка

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

Описание	Команда
Очищает статистику количества пакетов, отброшенных во время проверки IPv4 URPF	**clear ip urpf** [**interface** *interface-name*]

8.5.2. Отображение

Описание	Команда
Отображает конфигурацию и статистику IPv4 URPF	**show ip urpf** [**interface** *interface-name*]

8.5.3. Отладка

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

Описание	Команда
Отладка событий URPF	**debug urpf event**
Отладка таймеров URPF	**debug urpf timer**

9. НАСТРОЙКА CPP

9.1. Обзор

Политика защиты ЦП (CPP) предоставляет политики для защиты ЦП коммутатора.

В сетевых средах распространяются различные пакеты атак, которые могут вызвать высокую загрузку ЦП коммутаторов, повлиять на работу протокола и даже затруднить управление коммутатором. С этой целью процессоры коммутатора должны быть защищены, то есть управление трафиком и обработка на основе приоритетов должны выполняться для различных входящих пакетов, чтобы обеспечить возможности обработки процессоров коммутатора.

CPP может эффективно предотвращать злонамеренные атаки в сети и обеспечивать «беспрепятственную» среду для допустимых пакетов протоколов.

CPP включен по умолчанию. Обеспечивает защиту в течение всей эксплуатации коммутатора.

9.2. Приложения

Приложение	Описание
Предотвращение вредоносных атак	Когда в сеть проникают различные вредоносные атаки, такие как атаки ARP, CPP делит пакеты атаки на очереди с разным приоритетом, чтобы пакеты атаки не затрагивали другие пакеты
Предотвращение узких мест при обработке центральным процессором	Даже если атак нет, это может стать узким местом для ЦП при обработке избыточного нормального трафика. CPP может ограничивать скорость отправки пакетов на ЦП, чтобы обеспечить нормальную работу коммутаторов

9.2.1. Предотвращение вредоносных атак

9.2.1.1. Сценарий

Сетевые коммутаторы на всех уровнях могут быть атакованы вредоносными пакетами, как правило, атаками ARP.

Как показано на Рисунке 9-1, ЦП коммутатора обрабатывают три типа пакетов: forwarding-plane, control-plane и protocol-plane. Пакеты forwarding-plane используются для маршрутизации, включая пакеты ARP и пакеты отключения IP-маршрута. Пакеты control-plane используются для управления службами на коммутаторах, включая пакеты Telnet и пакеты HTTP. Пакеты protocol-plane служат для запуска протоколов, включая пакеты BPDU и пакеты OSPF.

Когда злоумышленник инициирует атаки с использованием пакетов ARP, пакеты ARP будут отправлены на ЦП для обработки. Поскольку процессор имеет ограниченные возможности обработки, пакеты ARP могут вытеснять другие пакеты (которые могут быть отброшены) и потреблять много ресурсов ЦП (для обработки пакетов атаки ARP). Следовательно, процессор не может нормально работать. В сценарии, показанном на Рисунке 9-1, возможные последствия включают в себя: обычные пользователи не могут получить доступ к сети; администраторы не могут управлять коммутаторами; канал OSPF

между коммутатором A и соседним устройством B отключен, и определение маршрута завершается ошибкой.

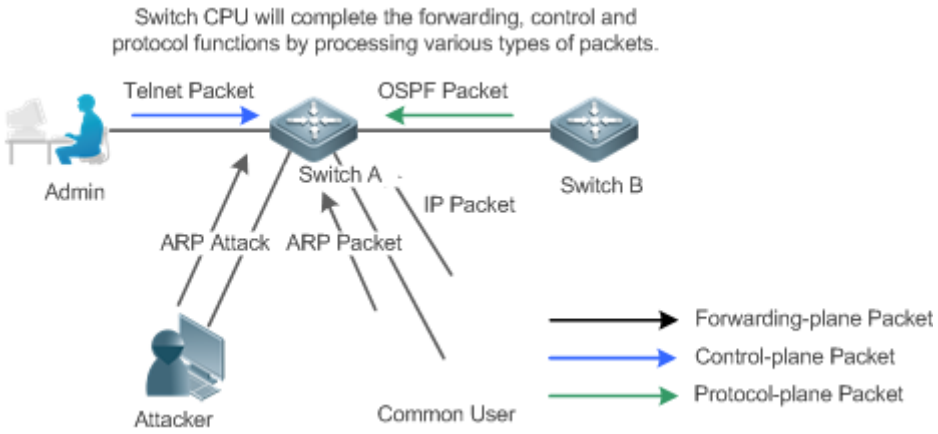


Рисунок 9-1. Сетевая топология коммутаторов и атак

9.2.1.2. Развертывание

- По умолчанию CPP классифицирует пакеты ARP, пакеты Telnet, пакеты отключения IP-маршрута и пакеты OSFP в очереди с разными приоритетами. Таким образом, пакеты ARP не будут влиять на другие пакеты.
- По умолчанию CPP ограничивает скорость пакетов ARP и скорость приоритетной очереди, в которой находятся пакеты ARP, чтобы гарантировать, что пакеты атаки не занимают слишком много ресурсов ЦП.
- Пакеты в той же очереди приоритета с пакетами ARP могут быть затронуты пакетами атаки ARP. Вы можете разделить пакеты и пакеты ARP на очереди с разным приоритетом с помощью конфигурации.
- Когда существуют пакеты атаки ARP, CPP не может предотвратить воздействие на обычные пакеты ARP. CPP может различать только тип пакета, но не может отличать атакующие пакеты от обычных пакетов того же типа. В этом случае можно использовать функцию Network Foundation Protection Policy (NFPP) для обеспечения более детального предотвращения атак.

ПРИМЕЧАНИЕ: описание конфигураций NFPP см. в разделе Настройка NFPP.

9.2.2. Предотвращение узких мест при обработке центральным процессором

9.2.2.1. Сценарий

Несмотря на отсутствие атак, может потребоваться одновременная отправка множества пакетов на ЦП для обработки.

Например, количество обращений к основному устройству кампусной сети исчисляется десятками тысяч. Трафик обычных пакетов ARP может достигать десятков тысяч пакетов в секунду (пак/с). Если все пакеты отправляются на ЦП для обработки, ресурсы ЦП не могут поддерживать обработку, что может привести к нестабильности (flapping) протокола и ненормальной работе ЦП.

9.2.2.2. Развертывание

- По умолчанию функция CPP ограничивает скорость пакетов ARP и скорость приоритетной очереди, в которой находятся пакеты APR, чтобы контролировать скорость пакетов ARP, отправляемых в ЦП, и гарантировать, что потребление

ресурсов ЦП находится в пределах заданного диапазона и что ЦП может нормально обрабатывать другие протоколы.

- По умолчанию функция CPP также ограничивает скорость передачи других пакетов на уровне пользователя.

9.3. Функции

9.3.1. Базовые концепты

QOS, DiffServ

Качество службы (QoS) — это механизм сетевой безопасности, технология, используемая для решения проблем сетевых задержек и перегрузок.

DiffServ относится к модели дифференцированного обслуживания, которая представляет собой типичную модель, реализованную QoS для классификации потоков обслуживания для предоставления дифференцированных услуг.

Пропускная способность, Скорость

Полоса пропускания относится к максимально допустимой скорости передачи данных, которая относится к порогу скорости в этом документе. Пакеты, скорость которых превышает пороговое значение, будут отброшены.

Скорость указывает фактическую скорость передачи данных. Когда скорость пакетов превышает пропускную способность, пакеты выше порогового значения будут отбрасываться. Скорость должна быть равна или меньше пропускной способности.

Единицами пропускной способности и скорости в этом документе являются пакеты в секунду (пак/с).

L2, L3, L4

Структура пакетов иерархическая, основанная на модели TCP/IP.

L2 относится к заголовкам уровня 2, а именно к части инкапсуляции Ethernet; L3 относится к заголовкам уровня 3, а именно к части IP-инкапсуляции; L4 относится к заголовкам уровня 4, обычно к части инкапсуляции TCP/UDP.

Приоритетная очередь, SP

Пакеты кешируются внутри коммутатора, а пакеты в направлении вывода кешируются в очередях. Приоритетные очереди сопоставляются со строгими приоритетами (SP). Очереди не равны, но имеют разные приоритеты.

SP является своего рода алгоритмом планирования QoS. Когда в очереди с более высоким приоритетом есть пакеты, пакеты в этой очереди планируются первыми. Планирование относится к выбору пакетов из очередей для вывода и относится к выбору и отправке пакетов в ЦП в этом документе.

Интерфейс процессора

Перед отправкой пакетов ЦП коммутатор кеширует пакеты. Процесс отправки пакетов в ЦП аналогичен процессу вывода пакетов. Интерфейс ЦП является виртуальным интерфейсом. Когда пакеты отправляются в ЦП, пакеты будут выводиться из этого виртуального интерфейса. Приоритетные очереди и SP, упомянутые выше, основаны на интерфейсе ЦП.

9.3.2. Обзор

CPP защищает ЦП, используя стандартную модель QoS DiffServ.

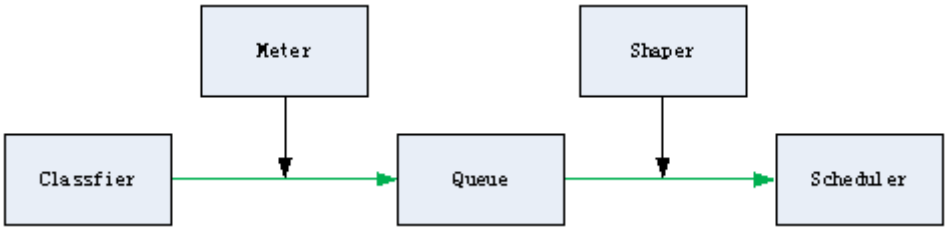


Рисунок 9-2. Модель реализации CPP

Особенность	Описание
Классификатор	Классифицирует типы пакетов и гарантирует последующую реализацию политик QoS
Измеритель	Ограничивает скорость на основе типов пакетов и контролирует пропускную способность для определенного типа пакетов
Очередь	Расставляет пакеты в очередь для отправки в ЦП и выбирает разные очереди на основе типов пакетов
Диспетчер	Выбирает и планирует очереди для отправки в ЦП
Шейпер	Выполняет ограничение скорости и управление пропускной способностью для приоритетных очередей и интерфейса ЦП

9.3.3. Классификатор

9.3.3.1. Принцип работы

Классификатор классифицирует все пакеты, которые должны быть отправлены в ЦП, на основе информации L2, L3 и L4 пакетов. Классификация пакетов является основой для реализации политик QoS. В последующих действиях реализуются различные политики на основе классификации для предоставления дифференцированных услуг. Коммутатор обеспечивает фиксированную классификацию. Функция управления классифицирует типы пакетов на основе протоколов, поддерживаемых коммутатором, например, пакеты STP BPDU и пакеты ICMP. Типы пакетов не могут быть настроены.

9.3.4. Измеритель

9.3.4.1. Принцип работы

Измеритель ограничивает скорость передачи различных пакетов на основе предварительно установленных пороговых значений скорости. Вы можете установить разные пороги скорости для разных типов пакетов. Когда скорость типа пакета превышает соответствующий порог, пакеты за пределами порога будут отбрасываться.

С помощью Измерителя вы можете контролировать скорость передачи типа пакета в ЦП в пределах порогового значения, чтобы предотвратить значительное влияние пакетов определенных атак на ресурсы ЦП. Это защита CPP уровня 1.

9.3.4.2. Связанная конфигурация

- По умолчанию каждый тип пакета соответствует порогу скорости (пропускной способности), и политики Измерителя реализуются на основе порога скорости.
- В приложении вы можете запустить команду **cpu-protect type** *packet-type* **bandwidth** *bandwidth-value*, чтобы установить политики Измерителя для указанных типов пакетов.

9.3.5. Очередь

9.3.5.1. Принцип работы

Очереди используются для классификации пакетов на уровне 2. Вы можете выбрать одну и ту же очередь для разных типов пакетов; Между тем, очереди кешируют пакеты внутри коммутаторов и предоставляют услуги Диспетчеру и Шейперу.

Очереди CPP являются очередями SP. SP пакетов определяются на основе времени их добавления в очередь. Пакеты с большим номером в очереди имеют более высокий приоритет.

9.3.5.2. Связанная конфигурация

- По умолчанию каждый тип пакета сопоставляется с очередью SP.
- В приложении вы можете запустить команду **cpu-protect type** *packet-type* **traffic-class** *traffic-class-num*, чтобы выбрать очереди SP для определенных типов пакетов.

9.3.6. Диспетчер

9.3.6.1. Принцип работы

Диспетчер планирует пакеты на основе SP очередей. То есть пакеты в очереди с более высоким приоритетом планируются первыми.

Перед планированием пакеты, которые должны быть отправлены в ЦП, кешируются в очередях. При планировании пакеты отправляются на ЦП для обработки.

ПРИМЕЧАНИЕ: поддерживается только политика планирования SP, которую нельзя изменить.

9.3.7. Шейпер

9.3.7.1. Принцип работы

Шейпер используется для формирования пакетов, которые должны быть отправлены в ЦП, то есть, когда фактическая скорость пакетов превышает порог формирования, пакеты должны оставаться в очереди и не могут быть запланированы. Когда скорость передачи пакетов колеблется, шейпер обеспечивает плавность скорости пакетов, отправляемых в ЦП (не выше порога шейпинга).

Когда Шейпер доступен, пакеты в очереди с более низким приоритетом могут быть добавлены в очередь до того, как будут добавлены в очередь все пакеты из очереди с более высоким приоритетом. Если скорость пакетов в очереди с определенным приоритетом превышает порог шейпинга, планирование пакетов в этой очереди может быть временно остановлено. Таким образом, Шейпер может предотвращать «голодание» пакетов в очередях с более низким приоритетом (когда планируются только пакеты в очередях с более высоким приоритетом, а пакеты в очередях с низким приоритетом не планируются).

Поскольку Шейпер ограничивает скорость планирования пакетов, он фактически выполняет функцию ограничения скорости. Шейпер обеспечивает ограничение скорости уровня 2 для приоритетных очередей и всех пакетов, отправляемых на ЦП (интерфейс ЦП). Функции Шейпера и счетчика обеспечивают 3-уровневое ограничение скорости вместе и обеспечивают защиту 3-го уровня для ЦП.

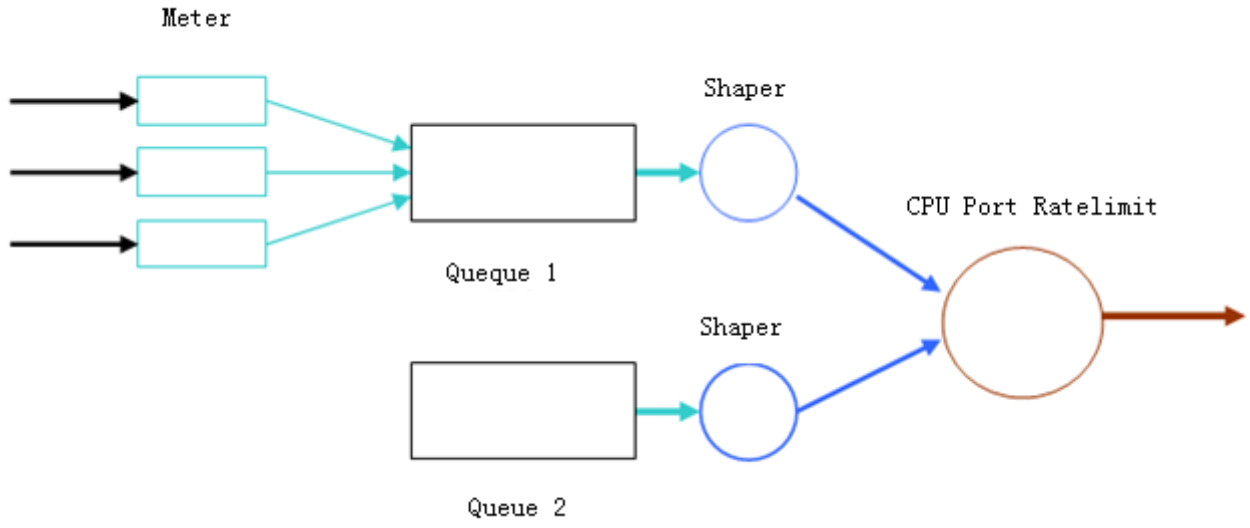


Рисунок 9-3. 3-уровневый предел скорости CPP

9.3.7.2. Связанная конфигурация

Настройка Шейпера для приоритетных очередей

- По умолчанию каждая приоритетная очередь определяет порог формирования (пропускную способность).
- В приложении вы можете запустить команду **cpu-protect traffic-class** *traffic-class-num* **bandwidth** *bandwidth_value*, чтобы выполнить настройку Шейпера для очереди с определенным приоритетом.

Настройка Шейпера для интерфейса CPU

- По умолчанию интерфейс ЦП определяет порог формирования (пропускную способность).
- Запустите команду **cpu-protect cpu bandwidth** *bandwidth_value*, чтобы выполнить настройку Шейпера для интерфейса ЦП.

9.4. Конфигурация

Конфигурация	Описание и команда	
Настройка CPP	(Опционально, настроено по умолчанию) Используется для настройки параметров конфигурации CPP	
	cpu-protect type *packet-type* **bandwidth**	Настраивает счетчик для типа пакета
	cpu-protect type *packet-type* **traffic-class**	Настраивает приоритетную очередь для типа пакета

Конфигурация	Описание и команда	
Настройка CPP	**cpu-protect traffic-class** *traffic-class-num* **bandwidth**	Настраивает Шейпер для приоритетной очереди
	cpu-protect cpu bandwidth	Настраивает Шейпер для интерфейса ЦП

9.4.1. Настройка CPP

9.4.1.1. Эффект конфигурации

- Настроив функцию Счетчика, вы можете установить ограничение пропускной способности и скорости для типа пакета. Пакеты за пределами лимита будут напрямую отбрасываться.
- Настроив функцию Очереди, вы можете выбрать приоритетную очередь для типа пакета. Пакеты в очереди с более высоким приоритетом будут запланированы первыми.
- Настроив функцию Шейпера, вы можете установить ограничение пропускной способности и скорости для интерфейса ЦП и приоритетной очереди. Пакеты за пределами лимита будут напрямую отбрасываться.

9.4.1.2. Примечания

- Обратите особое внимание, когда пропускная способность типа пакета установлена на меньшее значение, что может повлиять на обычный трафик того же типа. Чтобы обеспечить CPP для каждого пользователя, объедините функцию NFPP.
- Когда функции Счетчика и Шейпера объединены, будет обеспечена защита 3 уровня. Столкновения с защитой любого уровня сами по себе могут привести к негативным последствиям. Например, если вы хотите увеличить Счетчик типа пакета, также необходимо настроить Шейпер соответствующей приоритетной очереди. В противном случае пакеты этого типа могут повлиять на пакеты других типов в той же очереди приоритетов.

9.4.1.3. Шаги настройки

Настройка Счетчика для типа пакета

- Вы можете использовать или изменить значение по умолчанию, но не можете отключить его.
- Вам необходимо изменить конфигурацию в следующих случаях: когда пакеты типа не являются атакующими, но отбрасываются, вам необходимо увеличить Измеритель этого типа пакета. Если атаки пакетного типа вызывают ненормальную работу ЦП, вам необходимо уменьшить Счетчик этого типа пакета.
- Эта конфигурация доступна на всех коммутаторах в сетевой среде.

Настройка приоритетной очереди для типа пакета

- Вы можете использовать или изменить значение по умолчанию, но не можете отключить его.
- Вам необходимо изменить конфигурацию в следующих случаях: когда атаки типа пакета вызывают ненормальную работу других пакетов в той же очереди, вы

можете поместить тип пакета в неиспользуемую очередь. Если тип пакета нельзя отбросить, но этот тип пакета находится в той же очереди, что и другие используемые типы пакетов, вы можете поместить этот тип пакета в очередь с более высоким приоритетом.

- Эта конфигурация доступна на всех коммутаторах в сетевой среде.

Настройка Шейпера для приоритетной очереди

- Вы можете использовать или изменить значение по умолчанию и не можете отключить его.
- Вам необходимо изменить конфигурацию в следующих случаях: если значение Измерителя типа пакета больше, что приводит к тому, что другие пакеты в соответствующей очереди приоритета не имеют достаточной пропускной способности, вам необходимо увеличить Шейпер для этой очереди приоритета. Если пакеты атаки помещаются в приоритетную очередь и никакие другие пакеты не используются, вам необходимо увеличить Шейпер этой приоритетной очереди.
- Эта конфигурация доступна на всех коммутаторах в сетевой среде.

Настройка Шейпера для интерфейса CPU

- Вы можете использовать или изменить значение по умолчанию и не можете отключить его.
- Не рекомендуется менять Шейпер интерфейса процессора.
- Эта конфигурация доступна на всех коммутаторах в сетевой среде.

9.4.1.4. Проверка

- Измените конфигурации, когда система работает ненормально, и просмотрите систему, работающую после модификации, чтобы проверить, вступили ли конфигурации в силу.
- Проверьте, действуют ли конфигурации, просмотрев соответствующие конфигурации и статистические значения. Дополнительные сведения см. в следующих командах.

9.4.1.5. Связанные команды

Настройка Измерителя для типа пакета

Команда	**cpu-protect type** *packet-type* **bandwidth** *bandwidth_value*
Описание параметров	*packet-type*: указывает тип пакета. Определены типы пакетов. *bandwidth_value*: устанавливает пропускную способность в пакетах в секунду (пак/с)
Командный режим	Режим глобальной конфигурации

Настройка приоритетной очереди для типа пакета

Команда	**cpu-protect type** *packet-type* **traffic-class** *traffic-class-num*
Описание параметров	*packet-type*: указывает тип пакета. Определены типы пакетов. *traffic-class-num*: определяет приоритетную очередь

Командный режим	Режим глобальной конфигурации

Настройка Шейпера для приоритетной очереди

Команда	**cpu -protect traffic-class** *traffic-class-num* **bandwidth** *bandwidth_value*
Описание параметров	*traffic-class-num*: определяет приоритетную очередь. *bandwidth_value*: Устанавливает пропускную способность в единицах пак/с
Командный режим	Режим глобальной конфигурации

Настройка Шейпера для интерфейса CPU

Команда	**cpu-protect cpu bandwidth** *bandwidth_value*
Описание параметров	*bandwidth_value*: Устанавливает пропускную способность в единицах пак/с
Командный режим	Режим глобальной конфигурации

9.4.1.6. Пример конфигурации

Предотвращение пакетных атак и нестабильности сети с помощью CPP

Сценарий	• В системе доступны потоки ARP, IP, OSPF, dot1x, VRRP, Telnet и ICMP. В текущих конфигурациях ARP и 802.1X находятся в очереди приоритетов 2; потоки IP, ICMP и Telnet находятся в приоритетной очереди 4; потоки OSPF находятся в приоритетной очереди 3; потоки VRRP находятся в приоритетной очереди 6. Измеритель для каждого типа пакетов составляет 10 000 пакетов в секунду; Шейпер для каждой приоритетной очереди — 20 000 пак/с; Шейпер для интерфейса CPU — 100 000 пак/с. • В системе существуют атаки ARP и атаки IP-сканирования, которые вызывают ненормальную работу системы, сбой аутентификации, сбой Ping, сбой управления и нестабильность OSPF
Шаги настройки	• Поместите пакеты атаки ARP в приоритетную очередь 1 и ограничьте пропускную способность для пакетов ARP или соответствующей приоритетной очереди. • Поместить пакеты OSPF в приоритетную очередь 5. • Поместите пакеты атаки с ошибкой IP Ping в приоритетную очередь 3 и ограничьте пропускную способность для IP-пакетов или соответствующей приоритетной очереди

	QTECH# configure terminal QTECH(config)# cpu-protect type arp traffic-class 1 QTECH(config)# cpu-protect type arp bandwidth 5000 QTECH(config)# cpu-protect type ospf traffic-class 5 QTECH(config)# cpu-protect type v4uc-route traffic-class 3 QTECH(config)# cpu-protect type traffic-class 3 bandwidth 5000 QTECH(config)# end
Проверка	Запустите команду **show cpu-protect**, чтобы просмотреть конфигурацию и статистику
	QTECH#show cpu-protect %cpu port bandwidth: 100000(pps) Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) ------------ ------------ --------- --------- 0 6000 0 0 1 6000 0 0 2 6000 0 0 3 6000 0 0 4 6000 0 0 5 6000 0 0 6 6000 0 0 7 6000 0 0 Packet Type Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) Total Total Drop ----------- ------------ ------------ --------- --------- bpdu 6 128 0 0 0 0 arp 1 3000 0 0 0 0 tpp 6 128 0 0 0 0 dot1x 2 1500 0 0 0 0 gvrp 5 128 0 0 0 0 rldp 5 128 0 0 0 0 lacp 5 256 0 0 0 0 rerp 5 128 0 0 0 0 reup 5 128 0 0 0 0 lldp 5 768 0 0 0 0 cdp 5 768 0 0 0 0

	dhcps	2	1500	0	0	0	0
	dhcps6	2	1500	0	0	0	0
	dhcp6-client	2	1500	0	0	0	0
	dhcp6-server	2	1500	0	0	0	0
	dhcp-relay-c	2	1500	0	0	0	0
	dhcp-relay-s	2	1500	0	0	0	0
	option82	2	1500	0	0	0	0
	tunnel-bpdu	2	128	0	0	0	0
	tunnel-gvrp	2	128	0	0	0	0
	unknown-v6mc	1	128	0	0	0	0
	xgv6-ipmc	1	128	0	0	0	0
	stargv6-ipmc	1	128	0	0	0	0
	unknown-v4mc	1	128	0	0	0	0
	xgv-ipmc	2	128	0	0	0	0
	stargv-ipmc	2	128	0	0	0	0
	udp-helper	1	128	0	0	0	0
	dvmrp	4	128	0	0	0	0
	igmp	2	1000	0	0	0	0
	icmp	3	1600	0	0	0	0
	ospf	4	2000	0	0	0	0
	ospf3	4	2000	0	0	0	0
	pim	4	1000	0	0	0	0
	pimv6	4	1000	0	0	0	0
	rip	4	128	0	0	0	0
	ripng	4	128	0	0	0	0
	vrrp	6	256	0	0	0	0
	vrrpv6	6	256	0	0	0	0
	ttl0	0	128	0	0	0	0
	ttl1	0	2000	0	0	0	0
	hop-limit	0	800	0	0	0	0
	local-ipv4	3	4000	0	0	0	0
	local-ipv6	3	4000	0	0	0	0
	v4uc-route	1	800	0	0	0	0
	v6uc-route	1	800	0	0	0	0
	rt-host	4	3000	0	0	0	0
	mld	2	1000	0	0	0	0

	nd-snp-ns-na	1	3000	0	0	0	0
	nd-snp-rs	1	1000	0	0	0	0
	nd-snp-ra-redirect	1	1000	0	0	0	0
	erps	5	128	0	0	0	0
	mpls-ttl0	4	128	0	0	0	0
	mpls-ttl1	4	128	0	0	0	0
	mpls-ctrl	4	128	0	0	0	0
	isis	4	2000	0	0	0	0
	bgp	4	2000	0	0	0	0
	cfm	5	512	0	0	0	0
	web-auth	2	2000	0	0	0	0
	fcoe-fip	4	1000	0	0	0	0
	fcoe-local	4	1000	0	0	0	0
	bfd	6	5120	0	0	0	0
	micro-bfd	6	5120	0	0	0	0
	micro-bfd-v6	6	5120	0	0	0	0
	dldp	6	3200	0	0	0	0
	other	0	4096	0	0	0	0
	trill	4	1000	0	0	0	0
	efm	5	1000	0	0	0	0
	ipv6-all	0	2000	0	0	0	0
	ip-option	0	800	0	0	0	0
	mgmt	-	4000	4	0	4639	0
	dns	2	200	0	0	0	0
	sdn	0	5000	0	0	0	0
	sdn_of_fetch	0	5000	0	0	0	0
	sdn_of_copy	0	5000	0	0	0	0
	sdn_of_trap	0	5000	0	0	0	0
	vxlan-non-uc	1	512	0	0	0	0
	local-telnet	3	1000	0	0	0	0
	local-snmp	3	1000	0	0	0	0
	local-ssh	3	1000	0	0	0	0

9.4.2. Настройка предупреждения CPP

9.4.2.1. Эффект конфигурации

- При настройке предупреждения CPP включается периодическое обнаружение для проверки того, не потеряны ли пакеты протокола или пакеты в очередях.

- Настроив предупреждение CPP о потере пакетов протокола, при потере пакетов протокола распечатываются журналы тревог.
- Настроив предупреждение CPP о потере пакетов в очереди, при потере пакетов в очереди распечатываются журналы тревог.

9.4.2.2. Шаги настройки

Включение предупреждения CPP и настройка временного интервала между двумя обнаружениями потери пакетов

- Вы можете запустить команду **cpp-warn warn-period** *value*, чтобы включить предупреждения CPP и настроить временной интервал между двумя обнаружениями потери пакетов.
- По умолчанию предупреждение CPP отключено.

Включение предупреждения CPP о потере пакетов протокола

- Вы можете запустить команду **cpp-warn type** *packet-type* **warn**, чтобы разрешить CPP уменьшать потерю пакетов протокола.
- По умолчанию предупреждение CPP о потере пакетов протокола отключено.

Включение предупреждения CPP о потере пакетов в очереди

- Вы можете запустить команду **cpp-warn traffic-class** *raffic-class-num* **warn**, чтобы включить предупреждение CPP о потере пакетов в очереди.
- По умолчанию CPP снижение потерь пакетов в очереди отключено.

9.4.2.3. Связанные команды

Настройка временного интервала между двумя обнаружениями потери пакетов

Команда	**cpp-warn warn-period** *value*
Описание параметров	*value*: указывает интервал между двумя обнаружениями потери пакетов в секундах. Значение по умолчанию равно 0, что означает, что это обнаружение отключено
Командный режим	Режим глобальной конфигурации

Включение предупреждения CPP о потере пакетов протокола

Команда	**cpp-warn type** *packet-type* **warn**
Описание параметров	*packet-type*: указывает тип пакета. Определены типы пакетов
Командный режим	Режим глобальной конфигурации

Включение предупреждения CPP о потере пакетов в очереди

Команда	**cpp-warn traffic-class** *traffic-class-num* **warn**
Описание параметров	*traffic-class-num*: определяет приоритетную очередь
Командный режим	Режим глобальной конфигурации

9.4.2.4. Пример конфигурации

Настройка предупреждения CPP

Шаги настройки	• RFC 2131: протокол динамического конфигурирования сервера • RFC 2132: параметры DHCP и расширения поставщика BOOTP
	QTECH# configure terminal QTECH(config)# cpp-warn warn-period 10 QTECH(config)# cpp-warn traffic-class 1 warn QTECH(config)# cpp-warn type arp warn
Проверка	Запустите команду **show run**, чтобы просмотреть конфигурацию
	QTECH# show run | inc cpp cpp-warn warn-period 10 cpp-warn type arp warn cpp-warn traffic-class 1 warn

9.5. Мониторинг

9.5.1. Очистка

Описание	Команда
Очищает статистику CPP	**clear cpu-protect counters** [**device** *device_num*]
Очищает статистику CPP на master-устройстве	**clear cpu-protect counters mboard**

9.5.2. Отображение

Описание	Команда
Отображает конфигурацию и статистику типа пакета	**show cpu-protect type** *packet-type* [**device** *device_num*]
Отображает конфигурацию и статистику приоритетной очереди	**show cpu-protect traffic-class** *traffic-class-num* [**device** *device_num*]
Отображает конфигурацию интерфейса ЦП	**show cpu-protect cpu**
Отображает все конфигурации и статистику на master-устройстве	**show cpu-protect {mboard | summary }**
Отображает все конфигурации и статистику CPP	**show cpu-protect** [**device** *device_num*]
Отображает статистику CPP интерфейса	**show cpu-protect statistics** [**interface** *interface-id*]
Отображает тип статистики CPP	**show cpu-protect statistics type** *packet-type*

ПРИМЕЧАНИЕ: предыдущие команды мониторинга доступны как на шасси, так и на кассетных устройствах в автономном режиме.

ПРИМЕЧАНИЕ: если значение **device** не указано, команда **clear** используется для очистки статистики всех узлов в системе, а команда **show** используется для отображения конфигураций на master-устройстве.

ПРИМЕЧАНИЕ: в автономном режиме параметр **device** недоступен.

10. НАСТРОЙКА DHCP SNOOPING

10.1. Обзор

DHCP snooping отслеживает интерактивные пакеты DHCP между клиентами и серверами для записи и мониторинга IP-адресов пользователей и фильтрации незаконных пакетов DHCP, включая пакеты запросов клиентов и пакеты ответов сервера. Легальная база данных пользователей, созданная из записей DHCP Snooping, может обслуживать приложения безопасности, такие как IP Source Guard.

10.1.1. Протоколы и стандарты

- Определите, теряются ли пакеты протокола или пакеты в очередях каждые 10 секунд.
- Распечатывать журналы аварийных сигналов, если пакеты ARP потеряны.
- Распечатывать журналы аварийных сигналов, если пакеты в очереди 1 потеряны.

10.2. Приложения

Приложение	Описание
Защита от спуфинга службы DHCP	В сети с несколькими DHCP-серверами DHCP-клиентам разрешено получать сетевые конфигурации только от легальных DHCP-серверов
Защита от флудинга DHCP-пакетов	Злоумышленники могут часто отправлять пакеты DHCP-запросов
Защита от поддельных пакетов DHCP	Злоумышленники в сети могут отправлять поддельные пакеты DHCP-запросов, например, пакеты DHCP-RELEASE
Защита от спуфинга IP/MAC	Злоумышленники в сети могут отправлять поддельные IP-пакеты, например, поддельные поля исходного адреса пакетов
Предотвращение аренды IP-адресов	Пользователи сети могут арендовать IP-адреса, а не получать их с DHCP-сервера
Обнаружение ARP-атак	Злоумышленники подделывают пакеты ответов ARP для перехвата пакетов во время связи обычных пользователей

10.2.1. Защита от спуфинга службы DHCP

10.2.1.1. Сценарий

В сети может существовать несколько DHCP-серверов. Важно обеспечить, чтобы пользовательские ПК получали сетевые конфигурации только от DHCP-серверов в пределах контролируемой зоны.

Возьмем в качестве примера следующий Рисунок. DHCP-клиент может обмениваться данными только с доверенными DHCP-серверами.

- Пакеты запросов от DHCP-клиента могут передаваться только доверенным DHCP-серверам.
- Клиенту могут передаваться только ответные пакеты от доверенных DHCP-серверов.

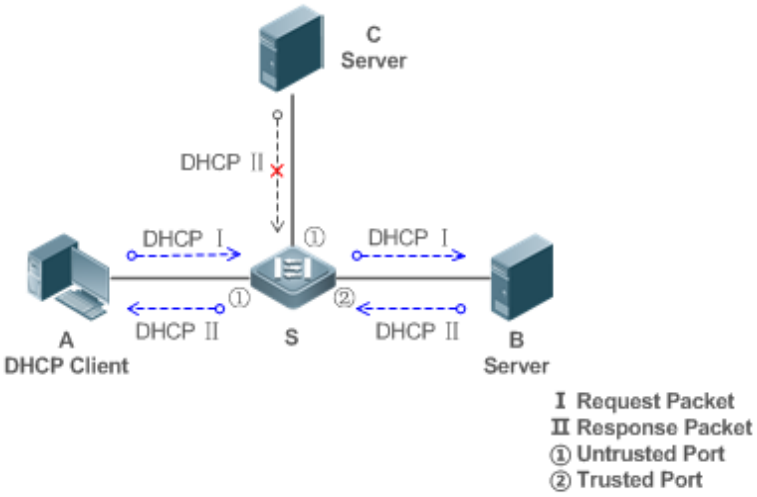


Рисунок 10-1.

S — устройство доступа.

A — пользовательский ПК.

B — DHCP-сервер в контролируемой зоне.

C — DHCP-сервер вне контролируемой зоны.

10.2.1.2. Развертывание

- Включите DHCP Snooping на S, чтобы реализовать мониторинг DHCP-пакетов.
- Установите порт на S, соединяющийся с B, как доверенный для передачи пакетов ответов.
- Установите остальные порты на S как ненадежные, чтобы фильтровать ответные пакеты.

10.2.2. Защита от флудинга DHCP-пакетов

10.2.2.1. Сценарий

Потенциальные вредоносные DHCP-клиенты в сети могут отправлять DHCP-пакеты с высокой скоростью. В результате законные пользователи не могут получить IP-адреса, а устройства доступа сильно загружены или даже выходят из строя. Необходимо принять меры для обеспечения стабильности сети.

С функцией ограничения скорости DHCP Snooping для пакетов DHCP клиент DHCP может отправлять пакеты запросов DHCP только со скоростью ниже ограничения.

- Пакеты запросов от DHCP-клиента отправляются со скоростью ниже лимита.
- Пакеты, отправленные со скоростью, превышающей лимит, будут отброшены.

10.2.2.2. Развертывание

- Включите DHCP Snooping на S, чтобы реализовать мониторинг DHCP.

- Ограничьте скорость пакетов DHCP с ненадежных портов.

10.2.3. Защита от поддельных пакетов DHCP

10.2.3.1. Сценарий

Потенциальные вредоносные клиенты в сети могут подделывать пакеты DHCP-запросов, потребляя применимые IP-адреса с серверов и, возможно, вытесняя IP-адреса легальных пользователей. Поэтому необходимо отфильтровывать нелегальные DHCP-пакеты.

Например, как показано на Рисунке ниже, будут проверяться пакеты DHCP-запросов, отправленные DHCP-клиентами.

- Поля MAC-адреса источника в пакетах запросов от клиентов DHCP должны совпадать с полями **chaddr** пакетов DHCP.
- Пакеты Release и Decline от клиентов должны совпадать с записями в базе данных привязок DHCP Snooping.

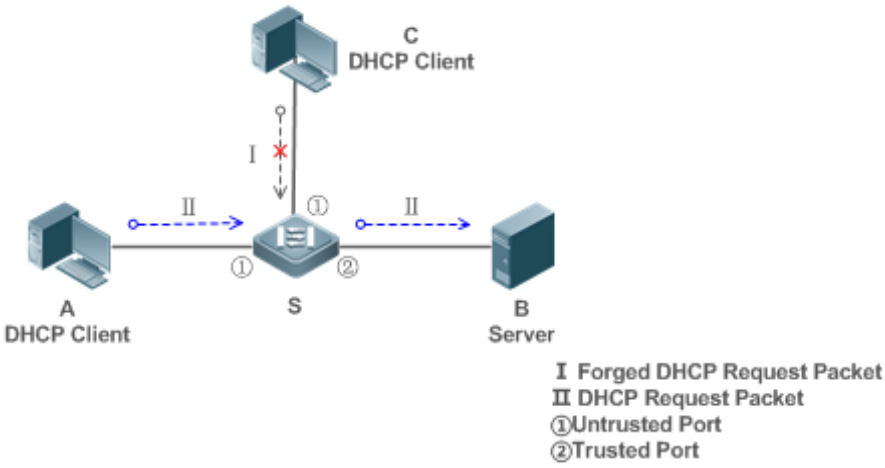


Рисунок 10-2.

S — устройство доступа.

A и C — пользовательские ПК.

B — DHCP-сервер в контролируемой зоне.

10.2.3.2. Развертывание

- Включите DHCP Snooping на S, чтобы реализовать мониторинг DHCP.
- Установите порт на S, соединяющийся с B, как доверенный для передачи пакетов ответов.
- Установите остальные порты на S как ненадежные, чтобы фильтровать ответные пакеты.
- Включите проверку исходного MAC-адреса DHCP Snooping на ненадежных портах S, чтобы отфильтровать нелегальные пакеты.

10.2.4. Защита от спуфинга IP/MAC

10.2.4.1. Сценарий

Проверяйте IP-пакеты из ненадежных портов, чтобы отфильтровать поддельные IP-пакеты на основе полей IP или IP-MAC.

Например, на следующем Рисунке IP-пакеты, отправленные DHCP-клиентами, проверяются.

- Поля исходного IP-адреса в IP-пакетах должны соответствовать IP-адресам, назначенным DHCP.
- Поля MAC-адреса источника в пакетах уровня 2 должны совпадать с полями **chaddr** в пакетах DHCP-запросов от клиентов.

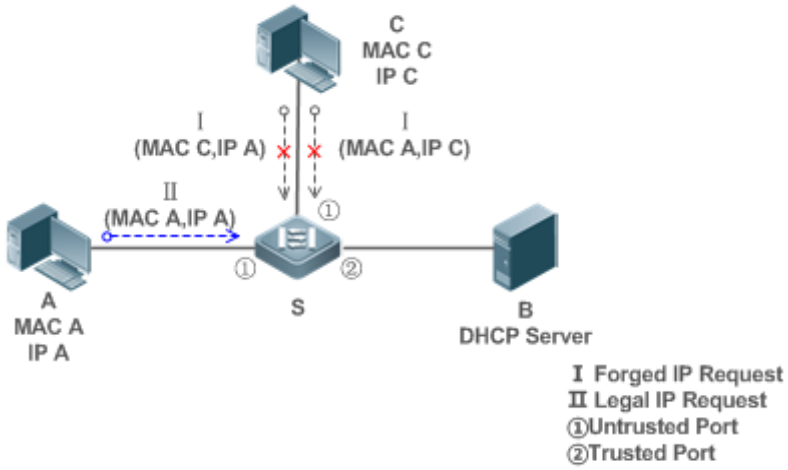


Рисунок 10-3.

S — устройство доступа.

A и C — пользовательские ПК.

B — DHCP-сервер в контролируемой зоне.

10.2.4.2. Развертывание

- Включите DHCP Snooping на S, чтобы реализовать мониторинг DHCP.
- Установите все downlink-порты на S как ненадежные DHCP Snooping.
- Включите IP Source Guard на S для фильтрации IP-пакетов.
- Включите IP Source Guard в режиме на основе IP-MAC, чтобы проверять поля исходного MAC-адреса и IP-адреса в IP-пакетах.

10.2.5. Предотвращение аренды IP-адресов

10.2.5.1. Сценарий

Проверяйте исходные адреса IP-пакетов из ненадежных портов по сравнению с адресами, назначенными DHCP.

Если исходные адреса, подключенные порты и исходные MAC-адреса портов уровня 2 в IP-пакетах не совпадают с назначениями DHCP-сервера, такие пакеты будут отброшены.

Сценарий топологии сети такой же, как показано на предыдущем Рисунке.

10.2.5.2. Развертывание

То же, что и в разделе «Защита от спуфинга IP/MAC».

10.2.6. Обнаружение ARP-атак

10.2.6.1. Сценарий

Проверяйте пакеты ARP от ненадежных портов и отфильтровывайте пакеты ARP, не соответствующие назначениям DHCP-сервера.

Например, на следующем Рисунке будут проверяться пакеты ARP, отправленные от DHCP-клиентов.

Порты, получающие пакеты ARP, MAC-адреса уровня 2 и исходные MAC-адреса отправителей пакетов ARP должны соответствовать истории DHCP Snooping.

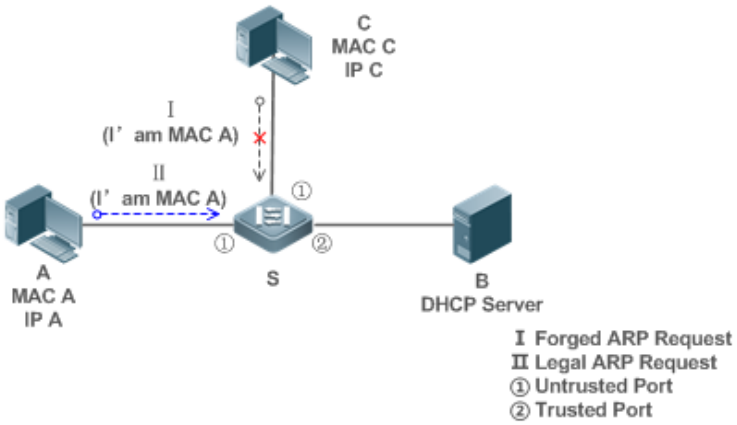


Рисунок 10-4.

S — устройство доступа.

A и C — пользовательские ПК.

B — DHCP-сервер в контролируемой зоне.

10.2.6.2. Развертывание

- Включите DHCP Snooping на S, чтобы реализовать мониторинг DHCP.
- Установите все downlink-порты на S как ненадежные.
- Включите IP Source Guard и ARP Check на всех ненадежных портах на S, чтобы реализовать фильтрацию пакетов ARP.

ПРИМЕЧАНИЕ: все вышеперечисленные функции управления безопасностью эффективны только для DHCP Snooping ненадежных портов.

10.3. Функции

10.3.1. Базовые концепты

Пакеты запросов DHCP

Пакеты запросов отправляются от DHCP-клиента на DHCP-сервер, включая пакеты DHCP-DISCOVER, пакеты DHCP-REQUEST, пакеты DHCP-DECLINE, пакеты DHCP-RELEASE и пакеты DHCP-INFORM.

Пакеты ответа DHCP

Пакеты ответа отправляются с DHCP-сервера на DHCP-клиент, включая пакеты DHCP-OFFER, пакеты DHCP-ACK и пакеты DHCP-NAK.

DHCP Snooping доверенных портов

Взаимодействие с запросом IP-адреса осуществляется через широковещательную рассылку. Следовательно, незаконные службы DHCP будут влиять на получение IP-адресов обычными клиентами и приведут к спуфингу и краже служб. Для предотвращения незаконных служб DHCP порты DHCP Snooping делятся на два типа: доверенные порты и ненадежные порты. Устройства доступа передают только пакеты ответа DHCP, полученные на доверенные порты, а такие пакеты от ненадежных портов отбрасываются. Таким образом, мы можем настроить порты, подключенные к легальному DHCP-серверу, как доверенные, а другие порты — как ненадежные, чтобы оградить нелегальные DHCP-серверы.

На коммутаторах все коммутационные порты или агрегированные порты уровня 2 по умолчанию считаются недоверенными, хотя можно указать доверенные порты.

Подавление пакетов DHCP Snooping

Чтобы защитить все пакеты DHCP на конкретном клиенте, мы можем включить подавление пакетов DHCP Snooping на его ненадежных портах.

DHCP Snooping на основе VLAN

DHCP Snooping может работать на основе VLAN. По умолчанию, когда DHCP Snooping включен, он действует для всех VLAN текущего клиента. Укажите VLAN, чтобы гибко контролировать эффективный диапазон DHCP Snooping.

База данных привязки DHCP Snooping

В сети DHCP клиенты могут устанавливать статические IP-адреса случайным образом. Это увеличивает не только сложность обслуживания сети, но и вероятность того, что легальные клиенты с IP-адресами, назначенными DHCP-сервером, могут не использовать сеть в обычном режиме из-за конфликта адресов. Отслеживая пакеты между клиентами и серверами, DHCP Snooping суммирует записи пользователей, включая IP-адреса, MAC-адреса, идентификатор VLAN (VID), порты и время аренды, для создания базы данных привязок DHCP Snooping. В сочетании с обнаружением и проверкой ARP DHCP Snooping контролирует надежное назначение IP-адресов легальным клиентам.

Ограничение скорости DHCP Snooping

Функция ограничения скорости DHCP Snooping может быть настроена с помощью команды ограничения скорости политики Network Foundation Protection Policy (NFPP). Для настройки NFPP см. Настройка NFPP.

DHCP Option82

DHCP Option82, опция для DHCP-пакетов, также называется DHCP Relay Agent Information Option. Поскольку номер опции равен 82, она известна как Option82. Option82 разработана для повышения безопасности DHCP-серверов и улучшения стратегий назначения IP-адресов. Этот параметр часто настраивается для служб DHCP Relay устройства доступа к сети, таких как DHCP Relay и DHCP Snooping. Этот параметр прозрачен для DHCP-клиентов, и компоненты DHCP Relay реализуют добавление и удаление этого параметра.

Нелегальные DHCP-пакеты

С помощью DHCP Snooping выполняется проверка пакетов DHCP, проходящих через клиента. Нелегальные пакеты DHCP отбрасываются, информация о пользователе записывается в базу данных привязок DHCP Snooping для дальнейших приложений

(например, обнаружение ARP). Следующие типы пакетов считаются недопустимыми DHCP-пакетами.

- Пакеты ответа DHCP, полученные на ненадежных портах, включая пакеты DHCP-ACK, DHCP-NACK и DHCP-OFFER.
- Пакеты DHCP-запросов, содержащие информацию о шлюзе **giaddr**, которые получены на ненадежных портах.
- Когда проверка MAC включена, пакеты с исходными MAC-адресами отличаются значением поля **chaddr** в DHCP-пакетах.
- Пакеты DHCP-RELEASE с записью в базе данных привязок DHCP Snooping, отслеживая при этом ненадежные порты, несовместимые с настройками в этой базе данных привязок.
- Пакеты DHCP имеют неправильный формат, или они неполные.

10.3.2. Обзор

Особенность	Описание
Фильтрация пакетов DHCP	Выполните проверку легальности DHCP-пакетов и отбросьте нелегальные пакеты (см. предыдущий раздел о нелегальных пакетах). Пакеты запросов на передачу принимаются только на доверенные порты
Создание базы данных привязок DHCP Snooping	Отслеживайте взаимодействие между DHCP-клиентами и сервером и создавайте базу данных привязок DHCP Snooping, чтобы обеспечить основу для других модулей фильтрации

10.3.3. Фильтрация пакетов DHCP

Выполните проверку пакетов DHCP с ненадежных портов. Отфильтруйте нелегальные пакеты, как описано в предыдущем разделе «Базовые концепты».

10.3.3.1. Принцип работы

Во время отслеживания проверяйте принимающие порты и поля пакетов, чтобы реализовать фильтрацию пакетов, и измените порты назначения пакетов, чтобы реализовать контроль диапазона передачи пакетов.

Проверка портов

При получении пакетов DHCP клиент сначала определяет, являются ли порты, принимающие пакеты, доверенными портами DHCP Snooping. Если да, проверка легальности и добавление записи привязки пропускаются, и пакеты передаются напрямую. Если нет, то нужны и проверка, и добавление.

Проверка инкапсуляции и длины пакета

Клиент проверяет, являются ли пакеты пакетами UDP и является ли порт назначения 67 или 68. Проверяет, соответствует ли длина пакета полю длины, определенному в протоколах.

Проверка полей и типов пакетов

В соответствии с типами нелегальных пакетов, представленными в разделе «Базовые концепты», проверьте поля **giaddr** и **chaddr** в пакетах, а затем проверьте, выполняются ли ограничительные условия для типа пакета.

10.3.3.2. Связанная конфигурация

Включение глобального DHCP Snooping

По умолчанию DHCP Snooping отключен.

Его можно включить на устройстве с помощью команды **ip dhcp snooping**.

Перед применением DHCP Snooping на основе VLAN необходимо включить глобальное DHCP Snooping.

Настройка DHCP Snooping на основе VLAN

По умолчанию, когда действует глобальное DHCP Snooping, DHCP Snooping действует для всех VLAN.

Используйте команду [**no**] **ip dhcp snooping vlan**, чтобы включить DHCP Snooping в указанных VLAN или удалить VLAN из указанных VLAN. Диапазон значений параметра команды — это фактический диапазон номеров VLAN.

Настройка проверки MAC-адреса источника DHCP Snooping

По умолчанию MAC-адреса пакетов уровня 2 и поля **chaddr** пакетов DHCP не проверяются.

Когда используется команда **ip dhcp snooping verify mac-address**, проверяются исходные MAC-адреса и поля **chaddr** пакетов запросов DHCP, отправленных с ненадежных портов. Пакеты запросов DHCP с разными MAC-адресами будут отброшены.

10.3.4. Создание базы данных привязок DHCP Snooping

DHCP Snooping обнаруживает интерактивные пакеты между DHCP-клиентами и DHCP-сервером и создает записи в базе данных привязок DHCP Snooping в соответствии с информацией о разрешенных DHCP-пакетах. Все эти допустимые записи предоставляются другим модулям безопасности клиента в качестве основы для фильтрации пакетов из сети.

10.3.4.1. Принцип работы

Во время отслеживания база данных привязок своевременно обновляется в зависимости от типов пакетов DHCP.

Создание записей привязки

Когда пакет DHCP-ACK на доверенном порту отслеживается, IP-адрес клиента, MAC-адрес и поле времени аренды извлекаются вместе с идентификатором порта (индексом проводного интерфейса) и идентификатором VLAN. Затем создается привязка к нему.

Удаление записей привязки

По истечении записанного времени аренды записи привязки она будет удалена, если отслеживается допустимый пакет DHCP-RELEASE/DHCP-DECLINE, отправленный клиентом, или пакет DHCP-NCK, полученный на доверенном порту, или команда **clear** использовалась.

10.3.4.2. Связанная конфигурация

Никакой настройки не требуется, кроме включения DHCP Snooping.

10.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций DHCP Snooping	(Обязательно) Используется для включения DHCP Snooping	
	ip dhcp snooping	Включает DHCP Snooping
	ip dhcp snooping suppression	Включает подавление пакетов DHCP Snooping
	ip dhcp snooping vlan	Включает DHCP Snooping на основе VLAN
	ip dhcp snooping verify mac-address	Настраивает проверку MAC-адреса источника DHCP Snooping
	ip dhcp snooping database write-delay	Периодически записывает базу данных привязки DHCP Snooping во флэш-память
	ip dhcp snooping database write-to-flash	Записывает базу данных привязки DHCP Snooping в файл резервной копии вручную
	renew ip dhcp snooping database	Импортирует флэш-память в базу данных привязки DHCP Snooping
	ip dhcp snooping trust	Настраивает доверенные порты DHCP Snooping
	ip dhcp snooping bootp	Включает поддержку BOOTP
	ip dhcp snooping check-giaddr	Включает DHCP Snooping для поддержки функции обработки запросов Relay
Настройка Option82	(Опционально) Используется для оптимизации назначения адресов DHCP-серверами	
	ip dhcp snooping Information option	Добавляет функции Option82 в пакеты запросов DHCP

Конфигурация	Описание и команда	
Настройка Option82	**ip dhcp snooping information option format remote-id**	Настраивает **remote-id** подопции Option82 в виде определяемой пользователем строки символов
	ip dhcp snooping information option format remote-id	Настраивает **circuit-id** подопции Option82 в виде определяемой пользователем строки символов

10.4.1. Настройка основных функций DHCP Snooping

10.4.1.1. Эффект конфигурации

- Включите DHCP Snooping.
- Создайте базу данных привязки DHCP Snooping.
- Управляйте диапазоном передачи DHCP-пакетов.
- Отфильтруйте нелегальные DHCP-пакеты.

10.4.1.2. Примечания

- Порты на клиентах, подключающихся к доверенному DHCP-серверу, должны быть настроены как доверенные.
- DHCP Snooping эффективно для портов проводной коммутации, агрегированных портов уровня 2 и подинтерфейсов инкапсуляции уровня 2. Конфигурация может быть реализована в режиме конфигурации интерфейса.
- DHCP Snooping и DHCP Relay являются взаимоисключающими в сценариях VRF.

10.4.1.3. Шаги настройки

Включение глобального DHCP Snooping

- Обязательный.
- Если не указано иное, эту функцию следует настроить на устройствах доступа.

Включение или отключение DHCP Snooping на основе VLAN

- DHCP Snooping можно отключить, если оно не требуется для некоторых VLAN.
- Если не указано иное, эту функцию следует настроить на устройствах доступа.

Настройка DHCP Snooping доверенных портов

- Обязательный.
- Настройте порты, соединяющие доверенный DHCP-сервер, как доверенные.

Включение проверки MAC-адреса источника DHCP Snooping

- Эта конфигурация требуется, если поля **chaddr** пакетов запросов DHCP совпадают с исходными MAC-адресами уровня 2 пакетов данных.
- Если не указано иное, эта функция должна быть включена на всех ненадежных портах устройств доступа.

Периодическая запись базы данных привязки DHCP Snooping во флэш-память

- Включите эту функцию, чтобы своевременно сохранять информацию базы данных привязок DHCP Snooping в случае перезагрузки клиента.
- Если не указано иное, эту функцию следует настроить на устройствах доступа.

Включение поддержки BOOTP

- Опционально
- Если не указано иное, эту функцию следует настроить на устройствах доступа.

Включение DHCP Snooping для обработки запросов Relay

- Опционально.
- Если не указано иное, эта функция должна быть включена на устройствах доступа.

10.4.1.4. Проверка

Настройте клиент для получения сетевых конфигураций по протоколу DHCP.

Проверьте, создается ли база данных привязок DHCP Snooping с записями на клиенте.

10.4.1.5. Связанные команды

Включение или отключение DHCP Snooping

Команда	**[no] ip dhcp snooping**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения глобального DHCP Snooping вы можете проверить DHCP Snooping с помощью команды **show ip dhcp snooping**

Настройка DHCP Snooping на основе VLAN

Команда	[**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }
Описание параметров	*vlan-rng*: указывает диапазон VLAN *vlan-min*: минимальный идентификатор VLAN *vlan-max*: максимальный идентификатор VLAN
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы включить или отключить DHCP Snooping в указанных VLAN. Эта функция доступна только после включения глобального DHCP Snooping

Настройка подавления пакетов DHCP Snooping

Команда	[**no**] **ip dhcp snooping suppression**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду, чтобы отклонить все пакеты DHCP-запросов на порту, то есть запретить всем пользователям под портом запрашивать адреса через DHCP

Настройка проверки MAC-адреса источника DHCP Snooping

Команда	[**no**] **ip dhcp snooping verify mac-address**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	При проверке исходного MAC-адреса MAC-адреса в заголовках каналов и полях CLIENT MAC в пакетах запросов, отправляемых DHCP CLIENT, проверяются на согласованность. Если проверка исходного MAC-адреса не удалась, пакеты будут отброшены

Периодическая запись базы данных DHCP Snooping на флэш-память

Команда	[**no**] **ip dhcp snooping database write-delay** [*time*]
Описание параметров	*time*: указывает интервал между двумя записями базы данных DHCP Snooping во флэш-память
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для записи базы данных DHCP Snooping в документ FLASH. Это позволяет избежать потери информации о привязке, которая требует повторного получения IP-адресов для возобновления связи после перезапуска устройства

Запись базы данных DHCP Snooping на флэш-память вручную

Команда	**ip dhcp snooping database write-to-flash**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для записи динамической информации о пользователе в базу данных DHCP Snooping в документах FLASH в режиме реального времени. Если устройство обновляется с версии, отличной от QinQ, до версии QinQ (или наоборот), записи привязки не могут быть восстановлены из документов FLASH из-за различий версий между документами FLASH

Импорт резервного хранилища файлов в базу данных привязки DHCP Snooping

Команда	**renew ip dhcp snooping database**
Командный режим	Привилегированный режим конфигурации
Руководство по использованию	Используйте эту команду, чтобы импортировать информацию из файла резервной копии в базу данных привязки DHCP Snooping

Настройка DHCP Snooping доверенных портов

Команда	[**no**] **ip dhcp snooping trust**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду, чтобы настроить порт, подключенный к легальному DHCP-серверу, в качестве доверенного порта. Пакеты ответов DHCP, полученные доверенными портами, передаются, а пакеты, полученные ненадежными портами, отбрасываются

Включение или отключение поддержки BOOTP

Команда	[**no**] **ip dhcp snooping bootp**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для поддержки протокола BOOPT

Включение DHCP Snooping для обработки запросов Relay

Команда	[**no**] **ip dhcp snooping check-giaddr**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения этой функции службы, использующие записи привязки DHCP Snooping, созданные на основе запросов Relay, такие как аутентификация IP Source Guard/802.1x, не могут быть развернуты. В противном случае пользователи не смогут получить доступ к Интернету. После включения этой функции нельзя использовать команду **ip dhcp snooping verify mac-address**. В противном случае запросы DHCP Relay будут отброшены, и в результате пользователи не смогут получить адреса

10.4.1.6. Пример конфигурации

DHCP-клиент, динамически получающий IP-адреса с легального DHCP-сервера

Сценарий:

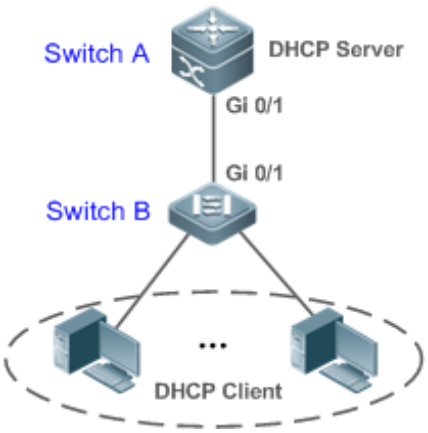


Рисунок 10-5.

Шаги настройки	• Включите DHCP Snooping на устройстве доступа (в данном случае на коммутаторе B). • Настройте uplink-порт (в данном случае порт Gi 0/1) как доверенный порт
B	B#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. B(config)#ip dhcp snooping B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust

	B(config-if-GigabitEthernet 0/1)#end
Проверка	Проверьте конфигурацию коммутатора B. • Проверьте, включено ли DHCP Snooping и является ли настроенный доверенный порт DHCP Snooping uplink. • Проверьте конфигурацию DHCP Snooping на коммутаторе B и особенно правильность доверенного порта
B	B#show running-config ! ip dhcp snooping ! interface GigabitEthernet 0/1 B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : DISABLE DHCP Snooping Support BOOTP bind status : DISABLE Interface Trusted Rate limit (pps) ---------- ------- ---------- GigabitEthernet 0/1 YES unlimited B#show ip dhcp snooping binding Total number of bindings: 1 MacAddress IpAddress Lease(sec) Type VLAN Interface ---------- ---------- ---------- ---------- ----- ------- 0013.2049.9014 172.16.1.2 86207 DHCP-Snooping 1 GigabitEthernet 0/11

10.4.1.7. Распространенные ошибки

- Uplink-порт не настроен как доверенный порт DHCP.
- Другой параметр безопасности доступа уже настроен для uplink-порта, поэтому нельзя настроить доверенный порт DHCP.

10.4.2. Настройка Option82

10.4.2.1. Эффект конфигурации

- Включите DHCP-сервер, чтобы получать больше информации и лучше назначать адреса.
- Функция Option 82 не зависит от клиента.

10.4.2.2. Примечания

Функции Opion82 для DHCP Snooping и DHCP Relay являются взаимоисключающими.

10.4.2.3. Шаги настройки

- Чтобы реализовать оптимизацию распределения адресов, выполните настройку.
- Если не указано иное, включите эту функцию на устройствах доступа с включенным DHCP Snooping.

10.4.2.4. Проверка

Проверьте, правильно ли настроены параметры конфигурации DHCP Snooping.

10.4.2.5. Связанные команды

Добавление Option82 в пакеты запросов DHCP

Команда	[**no**] **ip dhcp snooping information option** [**standard-format**]
Описание параметров	**standard-format**: указывает стандартный формат параметров Option82
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы добавить Option82 в пакеты запросов DHCP, чтобы DHCP-сервер назначал адреса в соответствии с этой информацией

Настройка подопции Option82 remote-id в виде определяемой пользователем строки символов

Команда	[**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname** }
Описание параметров	**string** *ASCII-string*: указывает, что содержимое расширяемого формата, опция Option82 **remote-id**, представляет собой определяемую пользователем строку символов. **hostname**: указывает, что содержимое расширяемого формата, опция **remote-id** Option82, является именем хоста
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для настройки удаленного идентификатора подопции Option82 в качестве определяемого пользователем содержимого, которое добавляется в пакеты запросов DHCP. Сервер DHCP назначает адреса в соответствии с информацией Option82

Конфигурация подопции Option82 circuit-id в виде определяемой пользователем строки символов

Команда	[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*
Описание параметров	*vlan-id*: указывает VLAN, в которой находится пакет запроса DHCP. *ascii-string*: указывает определяемую пользователем строку
Режим конфигурации	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду для настройки подопции Option82 **circuit-id** в качестве определяемого пользователем содержимого, которое добавляется в пакеты запросов DHCP. Сервер DHCP назначает адреса в соответствии с информацией Option82

10.4.2.6. Пример конфигурации

Настройка Option82 для пакетов запросов DHCP

Шаги настройки	Настройка основных функций DHCP Snooping. Настройка Option82
B	QTECH# configure terminal QTECH(config)# ip dhcp snooping information option QTECH(config)# end
Проверка	Проверьте конфигурацию DHCP Snooping
B	B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : ENABLE DHCP Snooping Support bootp bind status : DISABLE Interface Trusted Rate limit (pps) ---------- ------- ---------- GigabitEthernet 0/1 YES unlimited

10.5. Мониторинг

10.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд очистки может привести к потере жизненно важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает базу данных привязки DHCP Snooping	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]

10.5.2. Отображение

Описание	Команда
Отображает конфигурацию DHCP Snooping	**show ip dhcp snooping**
Отображает базу данных привязки DHCP Snooping	**show ip dhcp snooping binding**

10.5.3. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Отключите переключатель отладки сразу после использования.

Описание	Команда
Отладка событий DHCP Snooping	**debug snooping ipv4 event**
Отключает отладку событий DHCP Snooping	**no debug snooping ipv4 event**
Отладка пакетов DHCP Snooping	**debug snooping ipv4 packet**
Отключает отладку пакетов DHCP Snooping	**no debug snooping ipv4 packet**

11. НАСТРОЙКА NFPP

11.1. Обзор

Политика Network Foundation Protection Policy (NFPP) обеспечивает защиту коммутаторов.

Вредоносные атаки всегда обнаруживаются в сетевой среде. Эти атаки сильно нагружают коммутаторы, что приводит к высокой загрузке ЦП и проблемам в работе. Эти атаки заключаются в следующем:

Атаки типа «отказ в обслуживании» (DoS) могут потреблять много памяти, записей или других ресурсов коммутатора, что приведет к прекращению работы системной службы.

Массивный атакующий трафик направляется на ЦП, занимая всю пропускную способность ЦП. В этом случае обычный трафик протокола и трафик управления не могут быть обработаны ЦП, что приводит к нестабильности протокола или сбою управления. Пересылка в data plane также будет затронута, и вся сеть станет «ненормальной».

Большое количество атакующих пакетов, направленных на ЦП, потребляют огромные ресурсы ЦП, сильно нагружая ЦП и тем самым влияя на управление устройством и его производительность.

NFPP может эффективно защитить систему от этих атак. Сталкиваясь с атаками, NFPP поддерживает правильную работу различных системных служб с низкой загрузкой ЦП, тем самым обеспечивая стабильность всей сети.

11.2. Приложения

Приложение	Описание
Ограничение скорости атаки	Из-за различных вредоносных атак, таких как атаки ARP и атаки сканирования IP в сети, ЦП не может обрабатывать нормальный трафик протоколов и управления, вызывая нестабильность протокола или сбой управления. Функция ограничения скорости атаки NFPP используется для ограничения скорости трафика атаки или изоляции трафика атаки для восстановления сети
Централизованное распределение пропускной способности	Если трафик обычных служб слишком велик, вам необходимо классифицировать его и расставить приоритеты. Когда большое количество пакетов направляется в ЦП, центральный процессор будет сильно загружен, что приведет к сбою в управлении устройством или его запуске. Функция централизованного распределения полосы пропускания используется для повышения приоритета такого трафика, чтобы коммутаторы могли работать стабильно

11.2.1. Ограничение скорости атаки

11.2.1.1. Сценарий

NFPP поддерживает обнаружение атак и ограничение скорости для различных типов пакетов, включая пакеты протокола разрешения адресов (ARP), протокола управляющих

сообщений Интернета (ICMP) и протокола динамической конфигурации хоста (DHCP). Он также позволяет пользователям определять характеристики сопоставления пакетов и соответствующие политики обнаружения атак и ограничения скорости. Функция ограничения скорости атаки действует в зависимости от типов пакетов. В этом разделе пакеты ARP используются в качестве примера сценария для описания приложения.

Если злоумышленник рассылает пакеты атаки ARP, когда мощности ЦП недостаточно, большая часть ресурсов ЦП будет потребляться для обработки этих пакетов ARP. Если скорость пакетов ARP злоумышленника превышает максимальную пропускную способность ARP, указанную в политике защиты ЦП (CPP) коммутатора, обычные пакеты ARP могут быть отброшены. Как показано на Рисунке 11-1, обычные хосты не смогут получить доступ к сети, а коммутатор не сможет отправлять ответы ARP другим устройствам.

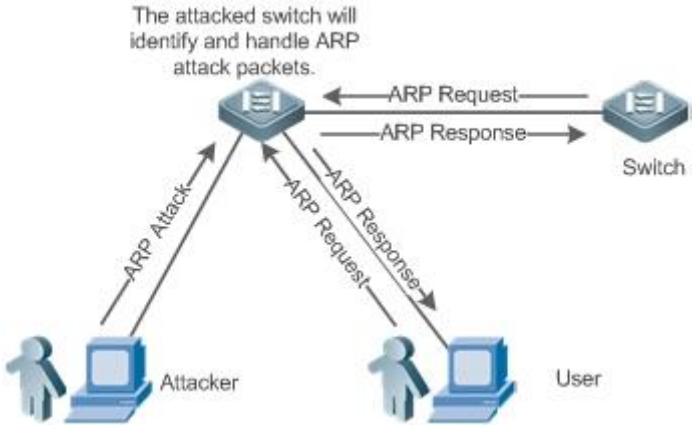


Рисунок 11-1.

11.2.1.2. Развертывание

- По умолчанию функция обнаружения атак ARP и ограничения скорости включена с настроенными соответствующими политиками. Если скорость пакетов ARP злоумышленника превышает ограничение скорости, пакеты отбрасываются. Если он превышает порог атаки, создается пользователь мониторинга и экспортируется подсказка.
- Если скорость пакетов ARP злоумышленника превышает предел скорости, определенный в CPP, и влияет на нормальные ответы ARP, вы можете включить изоляцию атаки, чтобы отклонить пакеты атаки ARP на основе оборудования и восстановить сеть.

ПРИМЕЧАНИЕ: дополнительные сведения о конфигурациях, связанных с CPP, см. в разделе Настройка защиты ЦП.

ПРИМЕЧАНИЕ: чтобы максимально использовать функции защиты NFPP, измените ограничения скорости различных служб в CPP в зависимости от среды приложения или используйте конфигурации, рекомендованные системой. Вы можете запустить команду **show cpu-protect summary**, чтобы отобразить конфигурации.

11.2.2. Централизованное распределение пропускной способности

11.2.2.1. Сценарий

Коммутатор классифицирует службы, определенные в CPP, по трем типам: управление (Manage), маршрут (Route) и протокол (Protocol). Каждый тип службы имеет независимую полосу пропускания. Различные типы служб не могут совместно использовать свои полосы пропускания. Трафик с пропускной способностью, превышающей пороговые значения,

будет отбрасываться. По такой классификации служб пакеты служб обрабатываются в порядке приоритета.

Как показано на Рисунке 11-2, коммутатор получает большое количество пакетов Telnet, пакетов OSPF и пакетов ARP, вызывая перегрузку ЦП. В этом случае ЦП не может обработать все пакеты, и большое количество пакетов задерживается в очереди, вызывая различные проблемы, такие как частое отключение Telnet, нестабильность протокола OSPF и сбой доступа ARP на хостах.

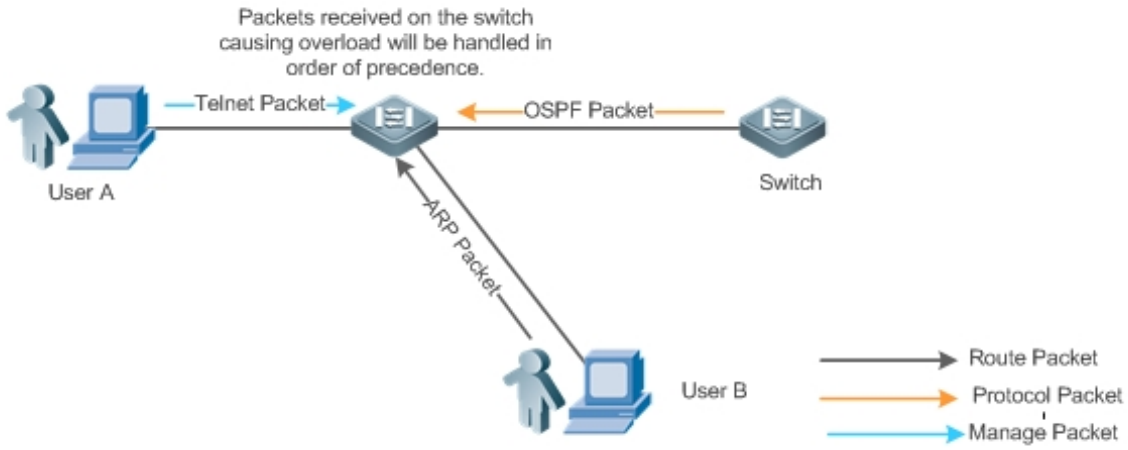


Рисунок 11-2.

11.2.2.2. Развертывание

- По умолчанию централизованное выделение полосы пропускания ЦП включено для назначения независимой полосы пропускания и коэффициента пропускной способности для каждого типа служб. В то время ЦП сначала обрабатывает пакеты Telnet, чтобы обеспечить бесперебойное подключение службы Telnet, затем обрабатывает пакеты OSPF для поддержания стабильности протокола OSPF и, наконец, обрабатывает пакеты ARP.
- Если описанные выше проблемы по-прежнему возникают в конфигурациях по умолчанию, вы можете соответствующим образом настроить пропускную способность и коэффициент пропускной способности для различных типов служб.

11.3. Функции

11.3.1. Базовые концепты

ARP Guard

В локальных сетях (LAN) IP-адреса сопоставляются с MAC-адресами через ARP, что играет важную роль в обеспечении безопасности сети. DoS-атаки на основе ARP означают, что на шлюз через сеть отправляется большое количество неавторизованных пакетов ARP, что приводит к отказу шлюза предоставлять услуги для обычных хостов. Чтобы предотвратить такие атаки, ограничьте скорость пакетов ARP, а также определите и изолируйте источник атаки.

IP Guard

Многие хакерские атаки и проникновения сетевых вирусов начинаются со сканирования активных хостов в сети. Поэтому многие сканируемые пакеты быстро занимают полосу пропускания сети, что приводит к сбою сетевого соединения.

Чтобы решить эту проблему, коммутаторы QTECH Layer-3 обеспечивают функцию IP Guard для предотвращения хакерского сканирования и вирусов Blaster Worm и снижения нагрузки на ЦП. В настоящее время существует два основных типа IP-атак:

Сканирование изменений IP-адреса назначения. Как самая большая угроза для сети, этот тип атак не только потребляет пропускную способность сети и увеличивает нагрузку на устройство, но также является предпосылкой к большинству хакерских атак.

Отправка IP-пакетов на несуществующие IP-адреса назначения с высокой скоростью: этот тип атак в основном предназначен для потребления нагрузки ЦП. Для устройства уровня 3, если существует IP-адрес назначения, пакеты пересылаются напрямую коммутационным чипом, не занимая ресурсы ЦП. Если IP-адрес назначения не существует, IP-пакеты отправляются на ЦП, который затем отправляет запросы ARP для запроса MAC-адреса, соответствующего IP-адресу назначения. Если на ЦП отправляется слишком много пакетов, ресурсы ЦП будут потребляться. Этот тип атаки менее разрушительный, чем первый.

Чтобы предотвратить последний тип атаки, ограничьте скорость IP-пакетов, а также найдите и изолируйте источник атаки.

ICMP Guard

ICMP — это распространенный подход к диагностике сетевых сбоев. После получения эхо-запроса ICMP от хоста маршрутизатор или коммутатор возвращает эхо-ответ ICMP. Предыдущий процесс требует, чтобы ЦП обрабатывал пакеты, тем самым определенно потребляя часть ресурсов ЦП. Если злоумышленник отправляет большое количество эхо-запросов ICMP на целевое устройство, огромные ресурсы ЦП на устройстве будут сильно потребляться, и устройство может даже не работать должным образом. Этот тип атак называется ICMP-флудом. Чтобы предотвратить атаки этого типа, ограничьте скорость пакетов ICMP, а также найдите и изолируйте источник атаки.

DHCP Guard

DHCP широко используется в локальных сетях для динамического назначения IP-адресов. Это важно для сетевой безопасности. В настоящее время наиболее распространенная атака DHCP, также называемая атакой исчерпания DHCP, использует поддельные MAC-адреса для широковещательной рассылки запросов DHCP. Различные инструменты атаки в Интернете могут легко завершить этот тип атаки. Сетевой злоумышленник может отправить достаточно запросов DHCP, чтобы использовать адресное пространство, предоставленное DHCP-сервером, в течение определенного периода времени. В этом случае авторизованные хосты не смогут запросить IP-адреса DHCP и, следовательно, не смогут получить доступ к сети. Чтобы предотвратить атаки этого типа, ограничьте скорость пакетов DHCP, а также найдите и изолируйте источник атаки.

DHCPv6 Guard

DHCP версии 6 (DHCPv6) широко используется в локальных сетях для динамического назначения адресов IPv6. И DHCP версии 4 (DHCPv4), и DHCPv6 имеют проблемы с безопасностью. Атаки на DHCPv4 применимы и к DHCPv6. Сетевой злоумышленник может отправить большое количество запросов DHCPv6, чтобы использовать адресное пространство, предоставленное сервером DHCPv6, в течение определенного периода времени. В этом случае авторизованные хосты не смогут запрашивать адреса IPv6 и, следовательно, не смогут получить доступ к сети. Чтобы предотвратить атаки этого типа, ограничьте скорость пакетов DHCPv6 и найдите источник атаки.

ND Guard

Обнаружение соседей (ND) в основном используется в сетях IPv6 для разрешения адресов, обнаружения маршрутизаторов, обнаружения префиксов и перенаправления. ND использует пять типов пакетов: запрос соседей (NS), объявление соседей (NA), запрос

маршрутизатора (RS), объявление маршрутизатора (RA) и перенаправление. Эти пакеты называются пакетами ND.

Self-Defined Guard

Существуют различные типы сетевых протоколов, в том числе протоколы маршрутизации, такие как протокол открытия кратчайшего пути (OSPF), протокол пограничного шлюза (BGP) и протокол информации о маршрутизации (RIP). Разным устройствам необходимо обмениваться пакетами по разным протоколам. Эти пакеты должны быть отправлены в ЦП и обработаны соответствующими протоколами. Как только сетевое устройство запускает протокол, это похоже на открытие окна для злоумышленников. Если злоумышленник отправляет большое количество протокольных пакетов на сетевое устройство, на устройстве будут потребляться огромные ресурсы ЦП, и, что еще хуже, устройство может работать неправильно.

Поскольку различные протоколы постоянно разрабатываются, используемые протоколы варьируются в зависимости от пользовательской среды. Таким образом, устройства QTECH обеспечивают самоопределяемую защиту. Пользователи могут настраивать и гибко настраивать типы защиты в соответствии с требованиями защиты в различных пользовательских средах.

11.3.2. Обзор

Особенность	Описание
Ограничение скорости на основе хоста и идентификация атак	Ограничивает скорость в соответствии с ограничением скорости на основе хоста и идентифицирует атаки хоста в сети
Ограничение скорости на основе портов и идентификация атак	Ограничивает скорость в соответствии с ограничением скорости на основе порта и идентифицирует атаки на порт
Период мониторинга	Отслеживает злоумышленников, атакующих хост в указанный период
Период изоляции	Использует аппаратное обеспечение для изоляции злоумышленников, атакующих хосты или порты в указанный период
Доверенные хосты	Доверяет хосту, не отслеживая его
Централизованное распределение пропускной способности	Классифицирует пакеты и приоритизирует их

11.3.3. Ограничение скорости на основе хоста и идентификация атак

Ограничьте скорость пакетов атак хостов и идентифицируйте атаки.

Определите сканирование ARP.

Определите IP-сканирование.

11.3.3.1. Принцип работы

Хосты можно идентифицировать двумя способами: на основе исходного IP-адреса, идентификатора VLAN, порта и на основе исходного MAC-адреса канального уровня, идентификатора VLAN и порта. У каждого хоста есть ограничение скорости и порог атаки (также называемый порогом тревоги). Ограничение скорости должно быть ниже порога атаки. Если скорость атакующих пакетов превышает ограничение скорости хоста, хост отбрасывает пакеты, превышающие ограничение скорости. Если скорость передачи пакетов атаки превышает порог атаки хоста, хост идентифицирует и регистрирует атаки хоста, а также отправляет trap-сообщения.

Атака со сканированием ARP могла произойти, если пакеты ARP, превышающие порог сканирования, полученные в настроенный период, соответствуют одному из следующих условий:

- MAC-адрес источника канального уровня является фиксированным, но IP-адрес источника изменяется.
- MAC-адрес источника канального уровня и IP-адрес источника являются фиксированными, но IP-адрес назначения постоянно меняется.

Среди IP-пакетов, превышающих порог сканирования, полученных в настроенный период, если IP-адрес источника остается неизменным, а IP-адрес назначения постоянно меняется, возможно, произошла атака сканирования IP.

ПРИМЕЧАНИЕ: когда NFPP обнаруживает определенный тип пакетов атаки в сервисе, он отправляет trap-сообщения администратору. Если трафик атаки сохраняется, NFPP не будет повторно отправлять сигнал тревоги до тех пор, пока не пройдет 60 секунд.

ПРИМЕЧАНИЕ: чтобы предотвратить потребление ресурсов ЦП, вызванное частой печатью журнала, NFPP записывает журналы обнаружения атак в буфер, получает их из буфера с заданной скоростью и распечатывает. NFPP не ограничивает количество trap-сообщений.

11.3.3.2. Связанные настройки

Используем ARP guard в качестве примера:

Настройка глобального ограничения скорости на основе хоста, порога атаки и порога сканирования

В режиме конфигурации NFPP:

Запустите команду **arp-guard rate-limit** {**per-src-ip** | **per-src-mac**} *pps* для настройки ограничений скорости для узлов, определенных на основе исходного IP-адреса, идентификатора VLAN, порта, и узлов, определенных на основе исходного MAC-адреса канального уровня, идентификатора VLAN и порта.

Запустите команду **arp-guard attack-threshold** {**per-src-ip** | **per-src-mac**} *pps* для настройки порогов атаки узлов, определенных на основе исходного IP-адреса, идентификатора VLAN, порта, и узлов, определенных на основе исходного MAC-адреса канального уровня, идентификатора VLAN и порта.

Запустите команду **arp-guard scan-threshold** *pkt-cnt*, чтобы настроить порог сканирования ARP.

Настройка ограничения скорости на основе хоста и порога атаки, а также порога сканирования на интерфейсе

В режиме настройки интерфейса:

Запустите команду **nfpp arp-guard policy** {**per-src-ip | per-src-mac**} *rate-limit-pps attack-threshold-pps* для настройки ограничений скорости и порогов атак для хостов,

идентифицированных на основе исходного IP-адреса, идентификатора VLAN и порта, а также хостов, идентифицированных на основе исходного MAC-адреса канального уровня, идентификатора VLAN и порта на интерфейсе.

Запустите команду **nfpp arp-guard scan-threshold** *pkt-cnt*, чтобы настроить порог сканирования на интерфейсе.

ПРИМЕЧАНИЕ: в настоящее время только RP guard и IP guard поддерживают антисканирование.

11.3.4. Ограничение скорости на основе портов и идентификация атак

11.3.4.1. Принцип работы

Каждый порт имеет ограничение скорости и порог атаки. Ограничение скорости должно быть ниже порога атаки. Если скорость передачи пакетов превышает ограничение скорости для порта, порт отбрасывает пакеты. Если скорость передачи пакетов превышает порог атаки на порт, порт регистрирует атаки и отправляет trap-сообщения.

11.3.4.2. Связанная конфигурация

Используем ARP guard в качестве примера:

Настройка глобального ограничения скорости на основе портов и порога атаки

В режиме конфигурации NFPP:

Запустите команду **arp-guard rate-limit per-port** *pps*, чтобы настроить ограничение скорости порта.

Запустите команду **arp-guard attack-threshold per-port** *pps*, чтобы настроить порог атаки порта.

Настройка ограничения скорости на основе порта и порога атаки на интерфейсе

В режиме настройки интерфейса:

Запустите команду **nfpp arp-guard policy per-port** *rate-limit-pps attack-threshold-pps*, чтобы настроить ограничение скорости и порог атаки порта.

11.3.5. Период мониторинга

11.3.5.1. Принцип работы

Пользователь мониторинга предоставляет информацию о злоумышленниках в текущей системе. Если период изоляции равен 0 (то есть не изолирован), модуль Guard автоматически выполняет программный мониторинг злоумышленников в настроенный период мониторинга. Если для периода изоляции установлено ненулевое значение, модуль защиты автоматически изолирует хосты, контролируемые программным обеспечением, и устанавливает период ожидания в качестве периода изоляции. Период мониторинга действителен, только если период изоляции равен 0.

11.3.5.2. Связанная конфигурация

Используем ARP guard в качестве примера:

Настройка периода глобального мониторинга

В режиме конфигурации NFPP:

Запустите команду **arp-guard monitor-period** *seconds*, чтобы настроить период мониторинга.

11.3.6. Период изоляции

11.3.6.1. Принцип работы

Изоляция выполняется с помощью защитных политик после обнаружения атак. Изоляция реализована с использованием аппаратного фильтра, чтобы гарантировать, что эти атаки не будут отправлены на центральный процессор, тем самым обеспечивая правильную работу устройства.

Аппаратная изоляция поддерживает два режима: изоляция на основе хоста и изоляция на основе порта. В настоящее время только ARP guard или ND guard поддерживает аппаратную изоляцию на основе портов.

В оборудовании настроена политика для изоляции злоумышленников. Однако аппаратные ресурсы ограничены. Когда аппаратные ресурсы израсходованы, система распечатывает журналы, чтобы уведомить об этом администратора.

11.3.6.2. Связанная конфигурация

Используем ARP guard в качестве примера:

Настройка периода глобальной изоляции

В режиме конфигурации NFPP:

Запустить команду **arp-guard isolate-period** [*seconds* | **permanent**] для настройки периода изоляции. Если для периода изоляции установлено значение 0, изоляция отключена. Если установлено ненулевое значение, это значение указывает период изоляции. Если установлено значение **permanent**, атаки ARP будут постоянно изолированы.

Настройка периода изоляции на интерфейсе

В режиме настройки интерфейса:

Запустите команду **nfpp arp-guard isolate-period** [*seconds* | **permanent**] для настройки периода изоляции. Если для периода изоляции установлено значение 0, изоляция отключена. Если установлено ненулевое значение, это значение указывает период изоляции. Если установлено значение **permanent**, атаки ARP будут постоянно изолированы.

Включение изолированной переадресации

В режиме конфигурации NFPP:

Запустите команду **arp-guard isolate-forwarding enable**, чтобы включить изолированную переадресацию.

Включение переадресации с ограничением скорости на основе порта

В режиме конфигурации NFPP:

Запустите команду **arp-guard ratelimit-forwarding enable**, чтобы включить переадресацию с ограничением скорости на основе порта.

ПРИМЕЧАНИЕ: в настоящее время только ARP guard поддерживает конфигурацию изолированной переадресации и переадресации с ограничением скорости.

11.3.7. Доверенные хосты

11.3.7.1. Принцип работы

Если вы не хотите отслеживать узел, вы можете запустить соответствующие команды, чтобы доверять узлу. Этому доверенному узлу будет разрешено отправлять пакеты на ЦП.

11.3.7.2. Связанная конфигурация

В качестве примера используйте антисканирование IP:

Настройка доверенных хостов

В режиме конфигурации NFPP:

Запустите команду **ip-guard trusted-host** *ip mask*, чтобы доверять хосту.

Запустите команду **trusted-host** {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}, чтобы доверить хосту Self-defined guard.

11.3.8. Централизованное распределение пропускной способности

11.3.8.1. Принцип работы

Службы, определенные в CPP, подразделяются на три типа: управление (Manage), маршрут (Route) и протокол(Protocol). (Подробнее см. в следующей таблице.) Каждый тип службы имеет независимую полосу пропускания. Различные типы служб не могут совместно использовать свои полосы пропускания. Трафик, превышающий пороги пропускной способности, отбрасывается. По такой классификации служб пакеты служб обрабатываются в порядке приоритета.

NFPP позволяет администратору гибко назначать полосу пропускания для трех типов пакетов в зависимости от фактической сетевой среды, чтобы пакеты протокола и управления могли быть обработаны в первую очередь. Предварительная обработка пакетов протоколов обеспечивает правильную работу протоколов, а предварительная обработка пакетов управления обеспечивает надлежащее управление для администратора, тем самым обеспечивая правильное выполнение важных функций устройства и улучшая возможности защиты устройства.

После классифицированного ограничения скорости все типы пакетов централизованно помещаются в очередь. Когда один тип службы обрабатывается неэффективно, пакеты этой службы будут задерживаться в очереди и могут в конечном итоге израсходовать ресурсы очереди. NFPP позволяет администратору настраивать процентное соотношение этих трех типов пакетов в очереди. Когда длина очереди, занятая одним типом пакетов, превышает значение общей длины очереди, умноженной на процент этого типа пакета, лишние пакеты будут отбрасываться. Это эффективно предотвращает исключительное использование ресурсов очереди одним типом пакетов.

Тип пакета	Тип услуги, определенный в CPP
Протокол (Protocol)	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, isis dhcps, gvrp, ripng,dvmrp, igmp, mpls, ospf, pim, pimv6, rip, vrrp, ospf3, dhcp-relay-s, dhcp-relay-c, option82, tunnel-bpdu, tunnel-gvrp
Маршрут (Route)	unknown-ipmc, unknown-ipmcv6, ttl1, ttl0, udp-helper, ip4-packet-other, ip6-packet-other, non-ip-packet-other, arp

Тип пакета	Тип услуги, определенный в CPP
Управление (Manage)	ip4-packet-local, ip6-packet-local

ПРИМЕЧАНИЕ: определения типов служб см. в разделе Настройка защиты ЦП.

11.3.8.2. Связанная конфигурация

Настройка максимальной пропускной способности указанных пакетов

В режиме глобальной конфигурации:

Запустите команду **cpu-protect sub-interface** { **manage** | **protocol**|**route**} **pps** *pps_value* для настройки максимальной пропускной способности указанных пакетов.

Настройка максимального процента указанных пакетов в очереди

В режиме глобальной конфигурации:

Запустите команду **cpu-protect sub-interface** { **manage** | **protocol** | **route**} **percent** *percent_value* для настройки максимального процента указанных пакетов в очереди.

11.4. Конфигурация

Конфигурация	Описание и команда	
Настройка ARP Guard	**arp-guard enable**	Глобально включает ARP guard
	arp-guard isolate-period	Настраивает глобальный период изоляции ARP guard
	arp-guard isolate-forwarding enable	Включает изолированную переадресацию ARP guard
	arp-guard ratelimit-forwarding enable	Включает переадресацию с ограничением скорости ARP guard
	arp-guard monitor-period	Настраивает глобальный период мониторинга ARP guard
	arp-guard monitored-host-limit	Настраивает максимальное количество хостов, контролируемых ARP guard
	arp-guard rate-limit	Настраивает глобальный предел скорости ARP guard
	arp-guard attack-threshold	Настраивает глобальный порог атаки ARP guard

Конфигурация	Описание и команда	
Настройка ARP Guard	**arp-guard scan-threshold**	Настраивает глобальный порог сканирования ARP guard
	nfpp arp-guard enable	Включает ARP guard на интерфейсе
	nfpp arp-guard policy	Настраивает ограничение скорости ARP guard и порог атаки на интерфейсе
	nfpp arp-guard scan-threshold	Настраивает порог сканирования APR guard на интерфейсе
	nfpp arp-guard isolate-period	Настраивает период изоляции APR guard на интерфейсе
Настройка IP Guard	**ip-guard enable**	Включает глобальную IP guard
	ip-guard isolate-period	Настраивает глобальный период изоляции IP guard
	ip-guard monitor-period	Настраивает период глобального мониторинга IP guard
	ip-guard monitored-host-limit	Настраивает максимальное количество хостов, контролируемых IP guard
	ip-guard rate-limit	Настраивает глобальный предел скорости IP guard
	ip-guard attack-threshold	Настраивает глобальный порог атаки IP guard
	ip-guard scan-threshold	Настраивает глобальный порог сканирования IP guard
	ip-guard trusted-host	Настраивает доверенные хосты IP guard
	nfpp ip-guard enable	Включает IP guard на интерфейсе

Конфигурация	Описание и команда	
Настройка IP Guard	**nfpp ip-guard policy**	Настраивает ограничение скорости IP guard и порог атаки на интерфейсе
	nfpp ip-guard scan-threshold	Настраивает порог сканирования IP guard на интерфейсе
	nfpp ip-guard isolate-period	Настраивает период изоляции IP guard на интерфейсе
Настройка ICMP Guard	**icmp-guard enable**	Глобально включает ICMP guard
	icmp-guard isolate-period	Настраивает глобальный период изоляции ICMP guard
	icmp-guard monitor-period	Настраивает период мониторинга глобальной ICMP guard
	icmp-guard monitored-host-limit	Настраивает максимальное количество хостов, контролируемых ICMP guard
	icmp-guard rate-limit	Настраивает глобальное ограничение скорости ICMP guard
	icmp-guard attack-threshold	Настраивает глобальный порог атаки ICMP guard
	icmp-guard trusted-host	Настраивает доверенные хосты ICMP guard
	nfpp icmp-guard enable	Включает ICMP guard на интерфейсе
	nfpp icmp-guard policy	Настраивает ограничение скорости ICMP guard и порог атаки на интерфейсе
	nfpp icmp-guard isolate-period	Настраивает период изоляции ICMP guard на интерфейсе
Настройка DHCP Guard	**dhcp-guard enable**	Включает глобальную DHCP guard

Конфигурация	Описание и команда	
Настройка DHCP Guard	**dhcp-guard isolate-period**	Настраивает глобальный период изоляции DHCP guard
	dhcp-guard monitor-period	Настраивает глобальный период мониторинга DHCP guard
	dhcp-guard monitored-host-limit	Настраивает максимальное количество хостов, контролируемых DHCP guard
	dhcp-guard rate-limit	Настраивает глобальный предел скорости DHCP guard
	dhcp-guard attack-threshold	Настраивает глобальный порог атаки DHCP guard
	nfpp dhcp-guard enable	Включает DHCP guard на интерфейсе
	nfpp dhcp-guard policy	Настраивает ограничение скорости DHCP guard и порог атаки на интерфейсе
	nfpp dhcp-guard isolate-period	Настраивает период изоляции DHCP guard на интерфейсе
Настройка DHCPv6 Guard	**dhcpv6-guard enable**	Включает глобальную DHCPv6 guard
	dhcpv6-guard monitor-period	Настраивает глобальный период мониторинга DHCPv6 guard
	dhcpv6-guard monitored-host-limit	Настраивает максимальное количество хостов, контролируемых DHCPv6 guard
	dhcpv6-guard rate-limit	Настраивает глобальное ограничение скорости DHCPv6 guard
	dhcpv6-guard attack-threshold { **per-src-mac | per-port**} *pps*	Настраивает глобальный порог атаки DHCPv6 guard

Конфигурация	Описание и команда	
Настройка DHCPv6 Guard	**nfpp dhcpv6-guard enable**	Включает DHCPv6 guard на интерфейсе
	nfpp dhcpv6-guard policy	Настраивает ограничение скорости DHCPv6 guard и порог атаки на интерфейсе
Настройка ND Guard	**nd-guard enable**	Глобально включает ND guard
	nd-guard ratelimit-forwarding enable	Включает переадресацию с ограничением скорости ND guard
	nd-guard rate-limit per-port	Настраивает глобальное ограничение скорости ND guard
	nd-guard attack-threshold per-port	Настраивает глобальный порог атаки ND guard
	nfpp nd-guard enable	Включает ND guard на интерфейсе
	nfpp nd-guard policy per-port	Настраивает ограничение скорости ND guard и порог атаки на интерфейсе
Настройка Self-Defined Guard	**define**	Настраивает имя Self-defined guard
	match	Настраивает поля **match** Self-defined guard
	global-policy	Настраивает глобальное ограничение скорости и порог атаки Self-defined guard
	monitor-period	Настраивает период глобального мониторинга Self-defined guard
	monitored-host-limit	Настраивает максимальное количество контролируемых хостов Self-defined guard
	trusted-host	Настраивает доверенные узлы Self-defined guard

Конфигурация	Описание и команда	
Настройка Self-Defined Guard	**define** *name* **enable**	Включает Self-defined guard глобально
	nfpp define *name* **enable**	Включает Self-defined guard на интерфейсе
	nfpp define	Настраивает ограничение скорости и порог атаки Self-defined guard на интерфейсе
Настройка ведения журнала NFPP	**log-buffer entries**	Настраивает размер буфера журнала
	log-buffer logs	Настраивает скорость буферизации журнала
	logging vlan	Настраивает фильтрацию журналов на основе VLAN
	logging interface	Настраивает фильтрацию журналов на основе интерфейса
	logging enable	Включает печать журнала

11.4.1. Настройка ARP Guard

11.4.1.1. Эффект конфигурации

- ARP-атаки идентифицируются на основе хостов или портов. Идентификация атаки ARP на основе хоста поддерживает два режима: идентификация на основе исходного IP-адреса, идентификатора VLAN и порта и идентификация на основе исходного MAC-адреса канального уровня, идентификатора VLAN и порта. Каждый тип идентификации атаки имеет ограничение скорости и порог атаки. Если скорость пакетов ARP превышает предел скорости, пакеты, превышающие предел скорости, отбрасываются. Если скорость пакетов ARP превышает порог атаки, система печатает информацию о тревоге и отправляет trap-сообщения. При идентификации атаки на основе хоста система также изолирует источник атаки.
- ARP guard также может обнаруживать атаки сканирования ARP. Атаки со сканированием ARP указывают на то, что исходный MAC-адрес канального уровня фиксирован, но исходный IP-адрес изменяется, или что исходный MAC-адрес канального уровня и исходный IP-адрес фиксированы, но IP-адрес назначения постоянно меняется. Из-за возможности ложного срабатывания хосты, которые могут выполнять сканирование ARP, не изолированы и предоставляются только для ссылки администратора.
- Настройте изоляцию ARP-guard для назначения аппаратно-изолированных записей против атак хоста, чтобы пакеты атаки не отправлялись на ЦП и не пересылались.

11.4.1.2. Примечания

- Для команды, настроенной как в режиме конфигурации NFPP, так и в режиме конфигурации интерфейса, конфигурация в режиме конфигурации интерфейса имеет приоритет над той, которая настроена в режиме конфигурации NFPP.
- Изоляция отключена по умолчанию. Если изоляция включена, злоумышленники займут аппаратные записи модуля безопасности.
- ARP guard предотвращает только DoS-атаки ARP на коммутатор, но не спуфинг ARP или атаки ARP в сети.
- Для доверенных портов, настроенных для динамической проверки ARP (DAI), ARP guard не действует, предотвращая ложное срабатывание трафика ARP через доверенные порты. Дополнительные сведения о доверенных портах DAI см. в разделе Настройка динамической проверки ARP.

11.4.1.3. Шаги настройки

Включение ARP guard

- (Обязательно) ARP guard включена по умолчанию.
- Эту функцию можно включить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если ARP guard отключена, система автоматически очищает отслеживаемые хосты, сканируемые хосты и изолированные записи на портах.

Настройка периода изоляции ARP Guard

- (Опционально) Изоляция ARP guard отключена по умолчанию.
- Если пакетный трафик злоумышленников превышает ограничение скорости, определенное в CPP, вы можете настроить период изоляции для отбрасывания пакетов и, следовательно, для экономии ресурсов полосы пропускания.
- Период изоляции можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются.

Включение изолированной переадресации ARP Guard

- (Опционально) Изолированная переадресация ARP guard включена по умолчанию.
- Чтобы сделать изоляцию действительной только в management plane, а не в forwarding plane, вы можете включить эту функцию.
- Эту функцию можно включить в режиме конфигурации NFPP.

Включение ограничения скорости переадресации ARP Guard

- (Опционально) Эта функция включена по умолчанию.
- Если вступает в силу запись изоляции на основе портов, вы можете включить эту функцию, чтобы пропускать некоторые пакеты, не отбрасывая их все.
- Эту функцию можно включить в режиме конфигурации NFPP.

Настройка периода мониторинга ARP Guard

- (Обязательно) Период мониторинга ARP guard по умолчанию составляет 600 секунд.
- Если настроен период изоляции ARP guard, он напрямую используется в качестве периода мониторинга, и настроенный период мониторинга теряет силу.

- Период мониторинга можно настроить в режиме конфигурации NFPP.

Настройка максимального количества хостов, контролируемых ARP Guard

- (Обязательно) По умолчанию максимальное количество хостов, контролируемых ARP guard, составляет 20 000.
- Разумно установите максимальное количество хостов, контролируемых ARP guard. По мере увеличения количества отслеживаемых хостов используется больше ресурсов ЦП.
- Максимальное количество хостов, контролируемых ARP guard, можно настроить в режиме конфигурации NFPP.
- Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts». Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить.
- Если таблица отслеживаемых хостов заполнена, система печатает журнал «% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.» для уведомления администратора.

Настройка порога атаки ARP Guard

- Обязательный.
- Для достижения наилучшего эффекта защиты ARP рекомендуется настроить ограничение скорости на основе хоста и порог атаки в следующем порядке: ограничение скорости на основе IP-адреса источника < порог атаки на основе IP-адреса источника < ограничение скорости на основе MAC-адреса источника < Порог атаки на основе MAC-адреса источника.
- Порог атаки можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если настроенное ограничение скорости больше порога атаки, система печатает журнал «%ERROR: rate limit is higher than attack threshold 500pps.», чтобы уведомить администратора.
- Если настроенный порог атаки меньше ограничения скорости, система печатает журнал «%ERROR: attack threshold is smaller than rate limit 300pps.», чтобы уведомить администратора.
- Если память не может быть выделена обнаруженным злоумышленникам, система печатает журнал «%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory.», чтобы уведомить администратора.
- Ограничение скорости на основе MAC-адреса источника имеет приоритет над ограничением скорости на основе IP-адреса источника, в то время как последнее имеет приоритет над ограничением скорости на основе порта.

Настройка порога сканирования ARP Guard

- Обязательный.
- Порог сканирования можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- В таблице сканирования ARP хранятся только последние 256 записей. Когда таблица сканирования ARP заполнена, последняя запись перезапишет самую раннюю запись.

- Атака со сканированием ARP могла произойти, если пакеты ARP, полученные в течение 10 секунд, соответствуют одному из следующих условий: MAC-адрес источника канального уровня фиксирован, но IP-адрес источника изменяется. MAC-адрес источника канального уровня и IP-адрес источника фиксируется, но IP-адрес назначения постоянно меняется, и время изменения превышает пороговое значение сканирования.

11.4.1.4. Проверка

Когда хост в сети отправляет пакеты атаки ARP на коммутатор, настроенный с ARP guard, проверьте, могут ли эти пакеты быть отправлены на ЦП.

- Если пакеты превышают порог атаки или порог сканирования, отображается журнал атак.
- Если для злоумышленника создается изолированная запись, отображается журнал изоляции.

11.4.1.5. Связанные команды

Глобальное включение ARP Guard

Команда	**arp-guard enable**
Командный режим	Режим конфигурации NFPP

Настройка глобального периода изоляции ARP Guard

Команда	**arp-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации NFPP

Включение изолированной переадресации ARP Guard

Команда	**arp-guard isolate-forwarding enable**
Командный режим	Режим конфигурации NFPP

Включение переадресации с порогом скорости ARP Guard

Команда	**arp-guard ratelimit-forwarding enable**
Командный режим	Режим конфигурации NFPP

Настройка глобального периода мониторинга ARP Guard

Команда	**arp-guard monitor-period** *seconds*
Описание параметров	*seconds*: указывает период мониторинга в секундах. Значение колеблется от 180 до 86 400
Командный режим	Режим конфигурации NFPP

Настройка максимального количества хостов, контролируемых ARP Guard

Команда	**arp-guard monitored-host-limit** *number*
Описание параметров	*number*: указывает максимальное количество отслеживаемых хостов в диапазоне от 1 до 4 294 967 295
Командный режим	Режим конфигурации NFPP

Настройка глобального ограничения скорости ARP Guard

Команда	**arp-guard rate-limit** {**per-src-ip** |**per-src-mac** | **per-port**} *pps*
Описание параметров	**per-src-ip**: ограничивает скорость каждого исходного IP-адреса. **per-src-mac**: ограничивает скорость каждого MAC-адреса источника. **per-port**: ограничивает скорость каждого порта. *pps*: указывает ограничение скорости в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Настройка глобального порога атаки ARP Guard

Команда	**arp-guard attack-threshold** {**per-src-ip** | **per-src-mac** | **per-port**} *pps*
Описание параметров	**per-src-ip**: настраивает порог атаки для каждого исходного IP-адреса. **per-src-mac**: настраивает порог атаки для каждого MAC-адреса источника. **per-port**: настраивает порог атаки для каждого порта. *pps*: указывает порог атаки в диапазоне от 1 до 19 999. Единицей является количество пакетов в секунду (пак/с)
Командный режим	Режим конфигурации NFPP

Руководство по использованию	Порог атаки должен быть равен или превышать порог скорости

Настройка глобального порога сканирования ARP Guard

Команда	**arp-guard scan-threshold** *pkt-cnt*
Описание параметров	*pkt-cnt*: указывает порог сканирования в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Включение ARP Guard на интерфейсе

Команда	**nfpp arp-guard enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	ARP Guard, настроенная в режиме конфигурации интерфейса, имеет приоритет над защитой, настроенной в режиме конфигурации NFPP

Настройка периода изоляции ARP Guard на интерфейсе

Команда	**nfpp arp-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. Значение 0 указывает на отсутствие изоляции. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации интерфейса

Настройка ограничения скорости ARP-Guard и порога атаки на интерфейсе

Команда	**nfpp arp-guard policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Описание параметров	**per-src-ip**: настраивает ограничение скорости и порог атаки для каждого исходного IP-адреса. **per-src-mac**: настраивает ограничение скорости и порог атаки для каждого MAC-адреса источника. **per-port**: настраивает ограничение скорости и порог атаки для каждого порта.

	rate-limit-pps: указывает ограничение скорости в диапазоне от 1 до 19999. *attack-threshold-pps*: указывает порог атаки в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

Настройка порога сканирования ARP Guard на интерфейсе

Команда	**nfpp arp-guard scan-threshold** *pkt-cnt*
Описание параметров	*pkt-cnt*: указывает порог сканирования в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса

11.4.1.6. Пример конфигурации

Защита ЦП на основе ARP Guard

Сценарий	• В системе существуют атаки узлов ARP, и некоторые узлы не могут правильно установить соединение ARP. • В системе существует сканирование ARP, вызывающее очень высокую загрузку ЦП
Шаги настройки	• Установите порог атаки на основе хоста на 5 пакетов в секунду. • Установите порог сканирования ARP на 10 пакетов в секунду. • Установите период изоляции на 180 пак/с
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#arp-guard rate-limit per-src-mac 5 QTECH (config-nfpp)#arp-guard attack-threshold per-src-mac 10 QTECH (config-nfpp)#arp-guard isolate-period 180
Проверка	Запустите команду **show nfpp arp-guard summary**, чтобы отобразить конфигурацию
	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-srcmac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold

	Global Disable 180 4/5/100 8/10/200 15 Maximum count of monitored hosts: 1000 Monitor period: 600s
	Запустите команду **show nfpp arp-guard hosts**, чтобы отобразить отслеживаемые хосты
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address MAC address remain-time(s) ---- --------- ---------- ---------- -------------- 1 Gi0/43 5.5.5.16 - 175 Total: 1 host
	Запустите команду **show nfpp arp-guard scan**, чтобы отобразить просканированные хосты
	VLAN interface IP address MAC address timestamp ---- --------- ---------- ---------- --------- 1 Gi0/5 - 08c6.b3c2.4609 2013-4-30 23:50:32 1 Gi0/5 192.168.206.2 08c6.b3c2.4609 2013-4-30 23:50:33 1 Gi0/5 - 08c6.b3c2.4609 2013-4-30 23:51:33 1 Gi0/5 192.168.206.2 08c6.b3c2.4609 2013-4-30 23:51:34 Total: 4 record(s)

11.4.2. Настройка IP Guard

11.4.2.1. Эффект конфигурации

- IP-атаки идентифицируются на основе хостов или физических интерфейсов. При идентификации IP-атак на основе хоста IP-атаки идентифицируются на основе исходного IP-адреса, идентификатора VLAN и порта. Каждый тип идентификации атаки имеет ограничение скорости и порог атаки. Если скорость передачи IP-пакетов превышает предел скорости, пакеты, превышающие предел скорости, отбрасываются. Если скорость передачи IP-пакетов превышает порог атаки, система распечатывает информацию о тревоге и отправляет trap-сообщения. При идентификации атаки на основе хоста система также изолирует источник атаки.
- IP Guard также может обнаруживать атаки сканирования IP. Антисканирование IP применяется к пакетным IP-атакам следующим образом: IP-адрес назначения постоянно меняется, но IP-адрес источника остается прежним, а IP-адрес назначения не является IP-адресом локального устройства.
- Настройте изоляцию IP guard, чтобы назначать аппаратно изолированные записи для защиты от атак хоста, чтобы пакеты атак не отправлялись на ЦП и не пересылались.

- Антисканирование IP-адресов применяется к атакам с использованием IP-пакетов, когда IP-адрес назначения не является локальным IP-адресом. CPP ограничивает скорость IP-пакетов, где IP-адрес назначения является локальным IP-адресом.

11.4.2.2. Примечания

- Для команды, настроенной как в режиме конфигурации NFPP, так и в режиме конфигурации интерфейса, конфигурация в режиме конфигурации интерфейса имеет приоритет над той, которая настроена в режиме конфигурации NFPP.
- Изоляция отключена по умолчанию. Если изоляция включена, злоумышленники займут аппаратные записи модуля безопасности.

11.4.2.3. Шаги настройки

Включение IP guard

- (Обязательно) IP guard включена по умолчанию.
- Эту функцию можно включить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если IP guard отключена, система автоматически очищает отслеживаемые хосты.

Настройка периода изоляции IP Guard

- (Необязательно) Изоляция IP guard по умолчанию отключена.
- Если пакетный трафик злоумышленников превышает ограничение скорости, определенное в CPP, вы можете настроить период изоляции для отбрасывания пакетов и, следовательно, для экономии ресурсов полосы пропускания.
- Период изоляции можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются.

Настройка периода мониторинга IP Guard

- (Обязательно) Период мониторинга IP guard по умолчанию составляет 600 секунд.
- Если настроен период изоляции IP Guard, он напрямую используется в качестве периода мониторинга, и настроенный период мониторинга теряет силу.
- Период мониторинга можно настроить в режиме конфигурации NFPP.

Настройка максимального количества хостов, контролируемых IP Guard

- (Обязательно) По умолчанию максимальное количество хостов, контролируемых IP Guard, составляет 20 000.
- Разумно установите максимальное количество хостов, контролируемых IP Guard. По мере увеличения количества отслеживаемых хостов используется больше ресурсов ЦП.
- Максимальное количество хостов, контролируемых IP Guard, можно настроить в режиме конфигурации NFPP.
- Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts.» Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить.

- Если таблица отслеживаемых хостов заполнена, система печатает журнал «% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.», чтобы уведомить администратора.

Настройка порога атаки IP Guard

- Обязательный.
- Порог атаки можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если настроенное ограничение скорости больше порога атаки, система печатает журнал «%ERROR: rate limit is higher than attack threshold 500pps.», чтобы уведомить администратора.
- Если настроенный порог атаки меньше ограничения скорости, система печатает журнал «%ERROR: attack threshold is smaller than rate limit 300pps.», чтобы уведомить администратора.
- Если память не может быть выделена обнаруженным злоумышленникам, система печатает журнал «%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory.», чтобы уведомить администратора.
- Ограничение скорости на основе исходного IP-адреса имеет приоритет над ограничением скорости на основе порта.

Настройка порога сканирования IP Guard

- Обязательный.
- Порог сканирования можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Атака со сканированием ARP могла произойти, если пакеты ARP, полученные в течение 10 секунд, соответствуют следующим условиям:
  - IP-адрес источника остается прежним.
  - IP-адрес назначения постоянно меняется и не является локальным IP-адресом, а время изменения превышает порог сканирования.

Настройка доверенных хостов IP Guard

- (Опционально) По умолчанию доверенный хост IP guard не настроен.
- Для IP Guard можно настроить не более 500 IP-адресов, которые не будут отслеживаться.
- Доверенные хосты можно настроить в режиме конфигурации NFPP.
- Если в таблице отслеживаемых хостов существует какая-либо запись, соответствующая доверенному хосту (IP-адреса совпадают), система автоматически удаляет эту запись.
- Если таблица доверенных хостов заполнена, система печатает журнал «%ERROR: Attempt to exceed limit of 500 trusted hosts."», чтобы уведомить администратора.
- Если доверенный хост не может быть удален, система печатает журнал «%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0.», чтобы уведомить администратора.
- Если хосту нельзя доверять, система печатает журнал «%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0.», чтобы уведомить администратора.
- Если хост, которому можно доверять, уже существует, система печатает журнал «%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured.», чтобы уведомить администратора.

- Если узел, который необходимо удалить из доверенной таблицы, не существует, система печатает журнал «%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found.», чтобы уведомить администратора.
- Если память не может быть выделена доверенному узлу, система печатает журнал «%ERROR: Failed to alloc memory.», чтобы уведомить администратора.

11.4.2.4. Проверка

Когда хост в сети отправляет пакеты IP-атаки на коммутатор, настроенный с IP Guard, проверьте, могут ли эти пакеты быть отправлены на ЦП.

- Если скорость пакетов от недоверенных хостов превышает порог атаки или порог сканирования, отображается журнал атаки.
- Если для злоумышленника создается изолированная запись, отображается журнал изоляции.

11.4.2.5. Связанные команды

Глобальное включение IP Guard

Команда	**ip-guard enable**
Командный режим	Режим конфигурации NFPP

Настройка глобального периода изоляции IP Guard

Команда	**ip-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации NFPP

Настройка глобального периода мониторинга IP Guard

Команда	**ip-guard monitor-period** *seconds*
Описание параметров	*seconds*: указывает период мониторинга в секундах. Значение колеблется от 180 до 86 400
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются

Настройка максимального количества хостов, контролируемых IP Guard

Команда	**ip-guard monitored-host-limit** *number*
Описание параметров	*number*: указывает максимальное количество отслеживаемых хостов в диапазоне от 1 до 4 294 967 295
Командный режим	Режим конфигурации NFPP

Настройка глобального ограничения скорости IP Guard

Команда	**ip-guard rate-limit** {**per-src-ip** | **per-port**} *pps*
Описание параметров	**per-src-ip**: ограничивает скорость каждого исходного IP-адреса. **per-port**: ограничивает скорость каждого порта. *pps*: указывает ограничение скорости в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Настройка глобального порога атаки IP Guard

Команда	**ip-guard attack-threshold** {**per-src-ip** | **per-port**} *pps*
Описание параметров	**per-src-ip**: настраивает порог атаки для каждого исходного IP-адреса. **per-port**: настраивает порог атаки для каждого порта. *pps*: указывает порог атаки в диапазоне от 1 до 19 999. Единица измерения — пак/с
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

Настройка глобального порога сканирования IP Guard

Команда	**ip-guard scan-threshold** *pkt-cnt*
Описание параметров	*pkt-cnt*: указывает порог сканирования в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Настройка доверенных хостов IP Guard

Команда	**ip-guard trusted-host** *ip mask*
Описание параметров	*ip*: указывает IP-адрес. *mask*: указывает маску IP-адреса. **all**: используется с **no** для удаления всех доверенных хостов
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если вы не хотите отслеживать хост, вы можете запустить эту команду, чтобы доверять хосту. Этот доверенный хост может отправлять IP-пакеты на ЦП без каких-либо ограничений скорости или сообщений о тревогах

Включение IP Guard на интерфейсе

Команда	**nfpp ip-guard enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	IP guard, настроенная в режиме конфигурации интерфейса, имеет приоритет над защитой, настроенной в режиме конфигурации NFPP

Настройка периода изоляции IP Guard на интерфейсе

Команда	**nfpp ip-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. Значение 0 указывает на отсутствие изоляции. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации интерфейса

Настройка ограничения скорости IP Guard и порога атаки на интерфейсе

Команда	**nfpp ip-guard policy** {**per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*
Описание параметров	**per-src-ip**: настраивает порог атаки для каждого исходного IP-адреса. **per-port**: настраивает порог атаки для каждого порта. *rate-limit-pps*: указывает ограничение скорости в диапазоне от 1 до 19999.

	attack-threshold-pps: указывает порог атаки в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

Настройка порога сканирования IP Guard на интерфейсе

Команда	**nfpp ip-guard scan-threshold** *pkt-cnt*
Описание параметров	*pkt-cnt*: указывает порог сканирования в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса

11.4.2.6. Пример конфигурации

Защита ЦП на основе IP Guard

Сценарий	• В системе существуют атаки IP-хостов, и пакеты некоторых хостов не могут быть должным образом маршрутизированы и перенаправлены. • В системе существует сканирование IP-адресов, что приводит к очень высокой загрузке ЦП. • Пакетный трафик некоторых хостов в системе очень велик, и эти пакеты должны пройти
Шаги настройки	• Настройте порог атаки на основе хоста. • Настройте порог сканирования IP. • Установите для периода изоляции ненулевое значение. • Настройте доверенные хосты
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#ip-guard rate-limit per-src-ip 20 QTECH (config-nfpp)#ip-guard attack-threshold per-src-ip 30 QTECH (config-nfpp)#ip-guard isolate-period 180 QTECH (config-nfpp)#ip-guard trusted-host 192.168.201.46 255.255.255.255
Проверка	Запустите команду **show nfpp ip-guard summary**, чтобы отобразить конфигурацию

	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-srcmac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold Global Disable 180 20/-/100 30/-/200 100 Maximum count of monitored hosts: 1000 Monitor period: 600s
	Запустите команду **show nfpp ip-guard hosts**, чтобы отобразить отслеживаемые хосты
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address Reason remain-time(s) ---- --------- ---------- ------ -------------- 1 Gi0/5 192.168.201.47 ATTACK 160 Total: 1 host
	Запустите команду **show nfpp ip-guard trusted-host**, чтобы отобразить доверенные хосты
	IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s)

11.4.3. Настройка ICMP Guard

11.4.3.1. Эффект конфигурации

- Атаки ICMP идентифицируются на основе хостов или портов. При идентификации атак на основе хоста атаки ICMP идентифицируются на основе исходного IP-адреса, идентификатора VLAN и порта. Каждый тип идентификации атаки имеет ограничение скорости и порог атаки. Если скорость передачи пакетов ICMP превышает ограничение скорости, пакеты, превышающие ограничение скорости, отбрасываются. Если скорость передачи ICMP-пакетов превышает порог атаки, система распечатывает информацию о тревоге и отправляет trap-сообщения. При идентификации атаки на основе хоста система также изолирует источник атаки.
- Настройте изоляцию ICMP Guard для назначения аппаратно-изолированных записей против атак хоста, чтобы пакеты атаки не отправлялись на ЦП и не пересылались.

11.4.3.2. Примечания

- Для команды, настроенной как в режиме конфигурации NFPP, так и в режиме конфигурации интерфейса, конфигурация в режиме конфигурации интерфейса имеет приоритет над той, которая настроена в режиме конфигурации NFPP.
- Изоляция отключена по умолчанию. Если изоляция включена, злоумышленники займут аппаратные записи модуля безопасности.

11.4.3.3. Шаги настройки

Включение ICMP Guard

- (Обязательно) ICMP Guard включена по умолчанию.
- Эту функцию можно включить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если ICMP Guard отключена, система автоматически очищает отслеживаемые хосты.

Настройка периода изоляции ICMP Guard

- (Опционально) Изоляция ICMP Guard по умолчанию отключена.
- Если пакетный трафик злоумышленников превышает ограничение скорости, определенное в CPP, вы можете настроить период изоляции для отбрасывания пакетов и, следовательно, для экономии ресурсов полосы пропускания.
- Период изоляции можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются.

Настройка периода мониторинга ICMP Guard

- (Обязательно) Период мониторинга ICMP Guard по умолчанию составляет 600 секунд.
- Если настроен период изоляции ICMP Guard, он напрямую используется в качестве периода мониторинга, и настроенный период мониторинга теряет силу.
- Период мониторинга можно настроить в режиме конфигурации NFPP.

Настройка максимального количества хостов, контролируемых ICMP Guard

- (Обязательно) Максимальное количество хостов, контролируемых ICMP Guard, по умолчанию составляет 20 000.
- Разумно установите максимальное количество хостов, контролируемых ICMP Guard. По мере увеличения числа реально отслеживаемых хостов используется больше ресурсов ЦП.
- Максимальное количество хостов, контролируемых ICMP Guard, можно настроить в режиме конфигурации NFPP.
- Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts.». Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить.

- Если таблица отслеживаемых хостов заполнена, система печатает журнал «% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.», чтобы уведомить администратора.

Настройка порога атаки ICMP Guard

- Обязательный.
- Порог атаки можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если настроенное ограничение скорости больше порога атаки, система печатает журнал «%ERROR: rate limit is higher than attack threshold 500pps.», чтобы уведомить администратора.
- Если настроенный порог атаки меньше ограничения скорости, система печатает журнал «%ERROR: attack threshold is smaller than rate limit 300pps.», чтобы уведомить администратора.
- Если память не может быть выделена обнаруженным злоумышленникам, система печатает журнал «%NFPP_ICMP_GUARD-4-NO_MEMORY: Failed to alloc memory.», чтобы уведомить администратора.
- Ограничение скорости на основе исходного IP-адреса имеет приоритет над ограничением скорости на основе порта.

Настройка доверенных хостов ICMP Guard

- (Опционально) По умолчанию доверенный узел ICMP Guard не настроен.
- Для защиты ICMP можно настроить не более 500 IP-адресов, которые не будут отслеживаться.
- Доверенные хосты можно настроить в режиме конфигурации NFPP.
- Если в таблице отслеживаемых хостов существует какая-либо запись, соответствующая доверенному хосту (IP-адреса совпадают), система автоматически удаляет эту запись.
- Если таблица доверенных хостов заполнена, система печатает журнал «%ERROR: Attempt to exceed limit of 500 trusted hosts.», чтобы уведомить администратора.
- Если доверенный хост не может быть удален, система печатает журнал «%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0.», чтобы уведомить администратора.
- Если хосту нельзя доверять, система печатает журнал «%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0.», чтобы уведомить администратора.
- Если хост, которому можно доверять, уже существует, система печатает журнал «%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured.». чтобы уведомить администратора.
- Если узел, который необходимо удалить из доверенной таблицы, не существует, система печатает журнал «%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found.», чтобы уведомить администратора.
- Если память не может быть выделена доверенному узлу, система печатает журнал «%ERROR: Failed to alloc memory.», чтобы уведомить администратора.

11.4.3.4. Проверка

Когда хост в сети отправляет пакеты атаки ICMP на коммутатор, настроенный с ICMP Guard, проверьте, могут ли эти пакеты быть отправлены на ЦП.

- Если скорость пакетов от ненадежного хоста превышает порог атаки, отображается журнал атак.
- Если для злоумышленника создается изолированная запись, отображается журнал изоляции.

11.4.3.5. Связанные команды

Глобальное включение ICMP Guard

Команда	**icmp-guard enable**
Командный режим	Режим конфигурации NFPP

Настройка периода глобальной изоляции ICMP Guard

Команда	**icmp-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. Значение 0 указывает на отсутствие изоляции. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Период изоляции злоумышленника делится на два типа: период глобальной изоляции и период изоляции на основе порта (период локальной изоляции). Для порта, если период изоляции на основе порта не настроен, используется глобальный период изоляции; в противном случае используется период изоляции на основе порта

Настройка периода глобального мониторинга ICMP Guard

Команда	**icmp-guard monitor-period** *seconds*
Описание параметров	*seconds*: указывает период мониторинга в секундах. Значение колеблется от 180 до 86 400
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если период изоляции равен 0, система выполняет программный мониторинг обнаруженных злоумышленников. Период тайм-аута является периодом мониторинга. Если во время мониторинга программного обеспечения для периода изоляции установлено ненулевое значение, система автоматически выполняет аппаратную изоляцию от контролируемых злоумышленников и устанавливает

	период ожидания в качестве периода мониторинга. Период мониторинга действителен, только если период изоляции равен 0. Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются

Настройка максимального количества хостов, контролируемых ICMP Guard

Команда	**icmp-guard monitored-host-limit** *number*
Описание параметров	*number*: указывает максимальное количество отслеживаемых хостов в диапазоне от 1 до 4 294 967 295
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts.». Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить. Если таблица отслеживаемых хостов заполнена, система печатает журнал «% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.», чтобы уведомить администратора

Настройка глобального ограничения скорости ICMP Guard

Команда	**icmp-guard rate-limit** {**per-src-ip** | **per-port**} *pps*
Описание параметров	**per-src-ip**: ограничивает скорость каждого исходного IP-адреса. **per-port**: ограничивает скорость каждого порта. *pps*: указывает ограничение скорости в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Настройка глобального порога атаки ICMP Guard

Команда	**icmp-guard attack-threshold** {**per-src-ip** | **per-port**} *pps*
Описание параметров	**per-src-ip**: настраивает порог атаки для каждого исходного IP-адреса. **per-port**: настраивает порог атаки для каждого порта. *pps*: указывает порог атаки в диапазоне от 1 до 19 999. Единица измерения — пак/с

Командный режим	Режим конфигурации NFPP

Настройка доверенных хостов ICMP Guard

Команда	**icmp-guard trusted-host** *ip mask*
Описание параметров	*ip*: указывает IP-адрес. *mask*: указывает маску IP-адреса. **all**: используется с **no** для удаления всех доверенных хостов
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если вы не хотите отслеживать хост, вы можете запустить эту команду, чтобы доверять хосту. Этот доверенный хост может отправлять ICMP-пакеты на ЦП без каких-либо ограничений скорости или сообщения о тревоге. Маску можно настроить таким образом, чтобы ни один узел в одном сегменте сети не отслеживался. Вы можете настроить до 500 доверенных хостов

Включение ICMP Guard на интерфейсе

Команда	**nfpp icmp-guard enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	ICMP Guard, настроенная в режиме конфигурации интерфейса, имеет приоритет над защитой, настроенной в режиме конфигурации NFPP

Настройка периода изоляции ICMP Guard на интерфейсе

Команда	**nfpp icmp-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. Значение 0 указывает на отсутствие изоляции. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации интерфейса

Настройка ограничения скорости ICMP Guard и порога атаки на интерфейсе

Команда	**nfpp icmp-guard policy** {**per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*
Описание параметров	**per-src-ip**: настраивает ограничение скорости и порог атаки для каждого исходного IP-адреса. **per-port**: настраивает ограничение скорости и порог атаки для каждого порта. *rate-limit-pps*: указывает ограничение скорости в диапазоне от 1 до 19999. *attack-threshold-pps*: указывает порог атаки в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

11.4.3.6. Пример конфигурации

Защита ЦП на основе ICMP Guard

Сценарий	• В системе существуют атаки хостов ICMP, и некоторые хосты не могут успешно пропинговать устройства. • Пакетный трафик некоторых хостов в системе очень велик, и эти пакеты должны пройти
Шаги настройки	• Настройте порог атаки на основе хоста. • Установите для периода изоляции ненулевое значение. • Настройте доверенные хосты
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#icmp-guard rate-limit per-src-ip 20 QTECH (config-nfpp)#icmp-guard attack-threshold per-src-ip 30 QTECH (config-nfpp)#icmp-guard isolate-period 180 QTECH (config-nfpp)#icmp-guard trusted-host 192.168.201.46 255.255.255.255
Проверка	Запустите команду **show nfpp icmp-guard summary**, чтобы отобразить конфигурацию
	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-srcmac/per-port.)

	Interface Status Isolate-period Rate-limit Attack-threshold Global Disable 180 20/-/400 30/-/400 Maximum count of monitored hosts: 1000 Monitor period: 600s
	Запустите команду **show nfpp icmp-guard hosts**, чтобы отобразить отслеживаемые хосты
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address remain-time(s) ---- --------- ---------- -------------- 1 Gi0/5 192.168.201.47 160 Total: 1 host
	Запустите команду **show nfpp icmp-guard trusted-host**, чтобы отобразить доверенные хосты
	IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s)

11.4.4. Настройка DHCP Guard

11.4.4.1. Эффект конфигурации

- DHCP-атаки идентифицируются на основе хостов или портов. При идентификации атак на основе хоста DHCP-атаки идентифицируются на основе исходного IP-адреса канального уровня, идентификатора VLAN и порта. Каждый тип идентификации атаки имеет ограничение скорости и порог атаки. Если скорость передачи пакетов DHCP превышает предел скорости, пакеты, превышающие предел скорости, отбрасываются. Если скорость передачи пакетов DHCP превышает порог атаки, система распечатывает информацию о тревоге и отправляет trap-сообщения. При идентификации атаки на основе хоста система также изолирует источник атаки.
- Настройте изоляцию DHCP Guard для назначения аппаратно-изолированных записей против атак хоста, чтобы пакеты атаки не отправлялись на ЦП и не пересылались.

11.4.4.2. Примечания

- Для команды, настроенной как в режиме конфигурации NFPP, так и в режиме конфигурации интерфейса, конфигурация в режиме конфигурации интерфейса имеет приоритет над той, которая настроена в режиме конфигурации NFPP.

- Изоляция отключена по умолчанию. Если изоляция включена, злоумышленники займут аппаратные записи модуля безопасности.
- Для доверенных портов, настроенных для отслеживания DHCP, DHCP Guard не действует, предотвращая ложное срабатывание трафика DHCP на доверенных портах. Дополнительные сведения о доверенных портах для отслеживания DHCP см. в разделе «Настройка DHCP Snooping».

11.4.4.3. Шаги настройки

Включение DHCP Guard

- (Обязательно) DHCP Guard включена по умолчанию.
- Эту функцию можно включить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если DHCP Guard отключена, система автоматически очищает отслеживаемые хосты.

Настройка периода изоляции DHCP Guard

- (Опционально) Изоляция DHCP Guard отключена по умолчанию.
- Если пакетный трафик злоумышленников превышает ограничение скорости, определенное в CPP, вы можете настроить период изоляции для отбрасывания пакетов и, следовательно, для экономии ресурсов полосы пропускания.
- Период изоляции можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются.

Настройка периода мониторинга DHCP Guard

- (Обязательно) Мониторинг DHCP Guard включен по умолчанию.
- Если настроен период изоляции DHCP Guard, он напрямую используется в качестве периода мониторинга, и настроенный период мониторинга теряет силу.
- Период мониторинга можно настроить в режиме конфигурации NFPP.

Настройка максимального количества хостов, контролируемых DHCP Guard

- (Обязательно) По умолчанию максимальное количество хостов, контролируемых DHCP Guard, составляет 20 000.
- Разумно установите максимальное количество хостов, контролируемых DHCP Guard. По мере увеличения количества отслеживаемых хостов используется больше ресурсов ЦП.
- Максимальное количество хостов, контролируемых DHCP Guard, можно настроить в режиме конфигурации NFPP.
- Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts.". Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить.
- Если таблица отслеживаемых хостов заполнена, система печатает журнал «% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.», чтобы уведомить администратора.

Настройка порога атаки DHCP Guard

- Обязательный.
- Порог атаки можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если настроенное ограничение скорости больше порога атаки, система печатает журнал «%ERROR: rate limit is higher than attack threshold 500pps.», чтобы уведомить администратора.
- Если настроенный порог атаки меньше ограничения скорости, система печатает журнал «%ERROR: attack threshold is smaller than rate limit 300pps.», чтобы уведомить администратора.
- Если память не может быть выделена обнаруженным злоумышленникам, система печатает журнал «%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory.», чтобы уведомить администратора.
- Ограничение скорости на основе исходного MAC-адреса имеет приоритет над ограничением скорости на основе порта.

11.4.4.4. Проверка

- Когда хост в сети отправляет пакеты атаки DHCP на коммутатор, настроенный с DHCP Guard, проверьте, могут ли эти пакеты быть отправлены на ЦП.
- Если параметр пакетов превышает порог атаки, отображается журнал атаки.
- Если для злоумышленника создается изолированная запись, отображается журнал изоляции.

11.4.4.5. Связанные команды

Глобальное включение DHCP Guard

Команда	**dhcp-guard enable**
Командный режим	Режим конфигурации NFPP

Настройка глобального периода изоляции DHCP Guard

Команда	**dhcp-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. Значение 0 указывает на отсутствие изоляции. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Период изоляции злоумышленника делится на два типа: период глобальной изоляции и период изоляции на основе порта (период локальной изоляции). Для порта, если период изоляции на основе

	порта не настроен, используется глобальный период изоляции; в противном случае используется период изоляции на основе порта

Настройка глобального периода мониторинга DHCP Guard

Команда	**dhcp-guard monitor-period** *seconds*
Описание параметров	*seconds*: указывает период мониторинга в секундах. Значение колеблется от 180 до 86 400
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если период изоляции равен 0, система выполняет программный мониторинг обнаруженных злоумышленников. Период тайм-аута является периодом мониторинга. Если во время мониторинга программного обеспечения для периода изоляции установлено ненулевое значение, система автоматически выполняет аппаратную изоляцию от контролируемых злоумышленников и устанавливает период ожидания в качестве периода мониторинга. Период мониторинга действителен, только если период изоляции равен 0. Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются

Настройка максимального количества хостов, контролируемых DHCP Guard

Команда	**dhcp-guard monitored-host-limit** *number*
Описание параметров	*number*: указывает максимальное количество отслеживаемых хостов в диапазоне от 1 до 4 294 967 295
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts.". Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить. Если таблица отслеживаемых хостов заполнена, система печатает журнал «% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.», чтобы уведомить администратора

Настройка глобального ограничения скорости DHCP Guard

Команда	**dhcp-guard rate-limit** {**per-src-mac** | **per-port**} *pps*
Описание параметров	**per-src-mac**: ограничивает скорость каждого MAC-адреса источника. **per-port**: ограничивает скорость каждого порта. *pps*: указывает ограничение скорости в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Настройка глобального порога атаки DHCP Guard

Команда	**dhcp-guard attack-threshold** {**per-src-mac** | **per-port**} *pps*
Описание параметров	**per-src-mac**: настраивает порог атаки для каждого MAC-адреса источника. **per-port**: настраивает порог атаки для каждого порта. *pps*: указывает порог атаки в диапазоне от 1 до 19 999. Единица измерения — пак/с
Командный режим	Режим конфигурации NFPP

Включение DHCP Guard на интерфейсе

Команда	**nfpp dhcp-guard enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	DHCP Guard, настроенная в режиме конфигурации интерфейса, имеет приоритет над защитой, настроенной в режиме конфигурации NFPP

Настройка периода изоляции DHCP-Guard на интерфейсе

Команда	**nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]
Описание параметров	*seconds*: указывает период изоляции в секундах. Его можно установить на 0 или любое значение от 30 до 86 400. Значение 0 указывает на отсутствие изоляции. **permanent**: указывает на постоянную изоляцию
Командный режим	Режим конфигурации интерфейса

Настройка ограничения скорости DHCP Guard и порога атаки на интерфейсе

Команда	**nfpp dhcp-guard policy** {**per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Описание параметров	**per-src-ip**: настраивает ограничение скорости и порог атаки для каждого исходного IP-адреса. **per-port**: настраивает ограничение скорости и порог атаки для каждого порта. *rate-limit-pps*: указывает ограничение скорости в диапазоне от 1 до 19 999. *attack-threshold-pps*: указывает порог атаки в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

11.4.4.6. Пример конфигурации

Защита ЦП на основе DHCP Guard

Сценарий	В системе существуют атаки хоста DHCP, и некоторые хосты не могут запросить IP-адреса
Шаги настройки	• Настройте порог атаки на основе хоста. • Установите для периода изоляции ненулевое значение
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#dhcp-guard rate-limit per-src-mac 8 QTECH (config-nfpp)#dhcp-guard attack-threshold per-src-mac 16 QTECH (config-nfpp)#dhcp-guard isolate-period 180
Проверка	Запустите команду **show nfpp dhcp-guard summary**, чтобы отобразить конфигурацию
	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-srcmac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Global Disable 180 -/8/150 -/16/300 Maximum count of monitored hosts: 1000

	Monitor period: 600s
	Запустите команду **show nfpp dhcp-guard hosts**, чтобы отобразить отслеживаемые хосты
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ----------- -------------- *1 Gi0/5 08c6.b3c2.4609 160 Total: 1 host

11.4.5. Настройка DHCPv6 Guard

11.4.5.1. Эффект конфигурации

Атаки DHCPv6 идентифицируются на основе хостов или портов. При идентификации атак на основе хоста атаки DHCPv6 идентифицируются на основе исходного IP-адреса канального уровня, идентификатора VLAN и порта. Каждый тип идентификации атаки имеет ограничение скорости и порог атаки. Если скорость передачи пакетов DHCPv6 превышает ограничение скорости, пакеты, превышающие ограничение скорости, отбрасываются. Если скорость передачи пакетов DHCPv6 превышает порог атаки, система печатает информацию о тревоге и отправляет trap-сообщения.

11.4.5.2. Примечания

- Для команды, настроенной как в режиме конфигурации NFPP, так и в режиме конфигурации интерфейса, конфигурация в режиме конфигурации интерфейса имеет приоритет над той, которая настроена в режиме конфигурации NFPP.
- Изоляция отключена по умолчанию. Если изоляция включена, злоумышленники займут аппаратные записи модуля безопасности.
- Для доверенных портов, настроенных для отслеживания DHCPv6, защита DHCPv6 не действует, предотвращая ложное срабатывание трафика DHCPv6 на доверенных портах. Дополнительные сведения о доверенных портах для отслеживания DHCPv6 см. в разделе «Настройка отслеживания DHCPv6».

11.4.5.3. Шаги настройки

Включение DHCPv6 Guard

- (Обязательно) DHCPv6 Guard включена по умолчанию.
- DHCPv6 Guard может быть включена в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если DHCPv6 Guard отключена, система автоматически очищает отслеживаемые узлы.

Настройка периода мониторинга DHCPv6 Guard

- (Обязательно) Период мониторинга DHCPv6 Guard по умолчанию составляет 600 секунд.
- Если настроен период изоляции DHCPv6 Guard, он напрямую используется в качестве периода мониторинга, и настроенный период мониторинга не вступает в силу.

- Период мониторинга DHCPv6 Guard можно настроить в режиме конфигурации NFPP.

Настройка максимального количества хостов, контролируемых DHCPv6 Guard

- (Обязательно) По умолчанию максимальное количество хостов, контролируемых DHCPv6 Guard, составляет 20 000.
- Разумно установите максимальное количество хостов, контролируемых DHCPv6 Guard. По мере увеличения количества отслеживаемых хостов используется больше ресурсов ЦП.
- Максимальное количество хостов, контролируемых DHCPv6 Guard, можно настроить в режиме конфигурации NFPP.
- Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts.". Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить.
- Если таблица отслеживаемых хостов заполнена, система печатает журнал % NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.», чтобы уведомить администратора.

Настройка порога атаки DHCPv6 Guard

- Обязательный.
- Порог атаки DHCPv6 Guard можно настроить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.
- Если настроенное ограничение скорости больше порога атаки, система печатает журнал «%ERROR: rate limit is higher than attack threshold 500pps.», чтобы уведомить администратора.
- Если настроенный порог атаки меньше ограничения скорости, система печатает журнал «%ERROR: attack threshold is smaller than rate limit 300pps.», чтобы уведомить администратора.
- Если память не может быть выделена обнаруженным злоумышленникам, система печатает журнал «%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory.», чтобы уведомить администратора.
- Ограничение скорости на основе исходного MAC-адреса имеет приоритет над ограничением скорости на основе порта.

11.4.5.4. Проверка

Когда хост в сети отправляет пакеты атаки DHCPv6 на коммутатор, настроенный с DHCPv6 Guard, проверьте, могут ли эти пакеты быть отправлены на ЦП.

- Если параметр пакетов превышает порог атаки, отображается журнал атаки.
- Если для злоумышленника создается изолированная запись, отображается журнал изоляции.

11.4.5.5. Связанные команды

Глобальное включение DHCPv6 Guard

Команда	**dhcpv6-guard enable**
Командный режим	Режим конфигурации NFPP

Настройка глобального периода мониторинга DHCPv6 Guard

Команда	**dhcpv6-guard monitor-period** *seconds*
Описание параметров	*seconds*: указывает период мониторинга в секундах. Значение колеблется от 180 до 86 400
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если период изоляции равен 0, система выполняет программный мониторинг обнаруженных злоумышленников. Период тайм-аута является периодом мониторинга. Если во время мониторинга программного обеспечения для периода изоляции установлено ненулевое значение, система автоматически выполняет аппаратную изоляцию от контролируемых злоумышленников и устанавливает период ожидания в качестве периода мониторинга. Период мониторинга действителен, только если период изоляции равен 0. Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются

Настройка максимального количества хостов, контролируемых DHCPv6 Guard

Команда	**dhcpv6-guard monitored-host-limit** *number*
Описание параметров	*number*: указывает максимальное количество отслеживаемых хостов в диапазоне от 1 до 4 294 967 295
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts.". Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить.

	Если таблица отслеживаемых хостов заполнена, система печатает журнал «%NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts.», чтобы уведомить администратора

Настройка глобального ограничения скорости DHCPv6 Guard

Команда	**dhcpv6-guardrate-limit** { **per-src-mac** | **per-port**} *pps*
Описание параметров	**per-src-mac**: ограничивает скорость каждого MAC-адреса источника. **per-port**: ограничивает скорость каждого порта. *pps*: указывает ограничение скорости в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Настройка глобального порога атаки DHCPv6 Guard

Команда	**dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port**} *pps*
Описание параметров	**per-src-mac**: настраивает порог атаки для каждого MAC-адреса источника. **per-port**: настраивает порог атаки для каждого порта. *pps*: указывает порог атаки в диапазоне от 1 до 19 999. Единица измерения — пак/с
Командный режим	Режим конфигурации NFPP

Включение DHCPv6 Guard на интерфейсе

Команда	**nfpp dhcpv6-guard enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	DHCPv6 Guard, настроенная в режиме конфигурации интерфейса, имеет приоритет над защитой, настроенной в режиме конфигурации NFPP

Настройка ограничения скорости DHCP Guard и порога атаки на интерфейсе

Команда	**nfpp dhcpv6-guard policy** {**per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Описание параметров	**per-src-mac**: настраивает ограничение скорости и порог атаки для каждого исходного IP-адреса. **per-port**: настраивает ограничение скорости и порог атаки для каждого порта. *rate-limit-pps*: указывает ограничение скорости в диапазоне от 1 до 19999. *attack-threshold-pps*: указывает порог атаки в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

11.4.5.6. Пример конфигурации

Защита ЦП на основе DHCPv6 Guard

Сценарий	В системе существуют атаки хостов DHCPv6, и обнаружение соседей DHCPv6 не удается на некоторых хостах
Шаги настройки	Настройте порог атаки на основе хоста
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#dhcpv6-guard rate-limit per-src-mac 8 QTECH (config-nfpp)#dhcpv6-guard attack-threshold per-src-mac 16
Проверка	Запустите сводную команду **show nfpp dhcpv6-guard summary**, чтобы отобразить конфигурацию
	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-srcmac/per-port.) Interface Status Rate-limit Attack-threshold Global Disable -/8/150 -/16/300 Maximum count of monitored hosts: 1000 Monitor period: 600s

	Запустите команду **show nfpp dhcpv6-guard hosts**, чтобы отобразить отслеживаемые хосты
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ----------- -------------- *1 Gi0/5 08c6.b3c2.4609 160 Total: 1 host

11.4.6. Настройка ND Guard

11.4.6.1. Эффект конфигурации

- AR ND Guard классифицирует пакеты ND на три типа в зависимости от их назначения: 1. NS и NA; 2. PC; 3. PA и перенаправление (Redirect). Пакеты типа 1 используются для разрешения адресов. Пакеты типа 2 используются хостами для обнаружения шлюза. Пакеты типа 3 связаны с маршрутизацией: RA используются для объявления шлюза и префикса, а пакеты Redirect используются для объявления лучшего next hop.
- В настоящее время поддерживается только идентификация пакетной атаки ND на основе порта. Вы можете настроить ограничения скорости и пороги атаки для этих трех типов пакетов соответственно. Если скорость передачи пакетов ND превышает предел скорости, пакеты, превышающие предел скорости, отбрасываются. Если скорость передачи пакетов ND превышает порог атаки, система печатает журналы и отправляет trap-сообщения.

11.4.6.2. Примечания

Для команды, настроенной как в режиме конфигурации NFPP, так и в режиме конфигурации интерфейса, конфигурация в режиме конфигурации интерфейса имеет приоритет над той, которая настроена в режиме конфигурации NFPP.

11.4.6.3. Шаги настройки

Включение ND Guard

- (Обязательно) ND Guard включена по умолчанию.
- Эту функцию можно включить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.

Включение порога скорости переадресации ND Guard

- (Опционально) Эта функция включена по умолчанию.
- Если вступает в силу запись изоляции на основе портов, вы можете включить эту функцию, чтобы пропускать некоторые пакеты, не отбрасывая их все.
- Эту функцию можно включить в режиме конфигурации NFPP.

Настройка порога атаки ND Guard

- Обязательный.
- Порог атаки ND Guard можно включить в режиме конфигурации NFPP или в режиме конфигурации интерфейса.

- Если настроенное ограничение скорости больше порога атаки, система печатает журнал «%ERROR: rate limit is higher than attack threshold 500pps.», чтобы уведомить администратора.
- Если настроенный порог атаки меньше ограничения скорости, система печатает журнал «%ERROR: attack threshold is smaller than rate limit 300pps.», чтобы уведомить администратора.
- Если память не может быть назначена обнаруженным злоумышленникам, система печатает журнал «%NFPP_ND_GUARD-4-NO_MEMORY: Failed to alloc memory.», чтобы уведомить администратора.

11.4.6.4. Проверка

Когда хост в сети отправляет пакеты атаки ND на коммутатор, настроенный с ND Guard, проверьте, могут ли эти пакеты быть отправлены на ЦП.

- Если параметр пакетов превышает порог атаки, отображается журнал атаки.

11.4.6.5. Связанные команды

Глобальное включение ND Guard

Команда	**nd-guard enable**
Командный режим	Режим конфигурации NFPP

Включение порога скорости переадресации ND Guard

Команда	**nd-guard ratelimit-forwarding enable**
Командный режим	Режим конфигурации NFPP

Настройка глобального ограничения скорости ND Guard

Команда	**nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*
Описание параметров	**ns-na**: указывает на NS и NA. **rs**: обозначает RS. **ra-redirect**: указывает RA и пакеты перенаправления. *pps*: указывает ограничение скорости в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации NFPP

Настройка глобального порога атаки ND Guard

Команда	**nd-guard attack-threshold per-port**[**ns-na** | **rs** | **ra-redirect**] *pps*
Описание параметров	**ns-na**: указывает на NS и NA. **rs**: обозначает RS. **ra-redirect**: указывает RA и пакеты перенаправления. *pps*: указывает порог атаки в диапазоне от 1 до 19 999. Единица измерения — пак/с
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

Включение ND Guard на интерфейсе

Команда	**nfpp nd-guard enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	ND Guard, настроенная в режиме конфигурации интерфейса, имеет приоритет над защитой, настроенной в режиме конфигурации NFPP

Настройка ограничения скорости ND Guard и порога атаки на интерфейсе

Команда	**nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*
Описание параметров	**ns-na**: указывает на NS и NA. **rs**: обозначает RS. **ra-redirect**: указывает RA и пакеты перенаправления. *rate-limit-pps*: указывает ограничение скорости в диапазоне от 1 до 19999. *attack-threshold-pps*: указывает порог атаки в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

11.4.6.6. Пример конфигурации

Защита процессора на основе ND Guard

Сценарий	В системе существуют атаки узлов ND, и обнаружение соседей на некоторых узлах не удается
Шаги настройки	Настройте порог атаки на основе хоста
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)# nd-guard rate-limit per-port ns-na 30 QTECH (config-nfpp)# nd-guard attack-threshold per-port ns-na 50
Проверка	Запустите команду **show nfpp nd-guard summary**, чтобы отобразить конфигурацию
	(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.) Interface Status Rate-limit Attack-threshold Globa Disable 30/15/15

11.4.7. Настройка Self-Defined Guard

11.4.7.1. Эффект конфигурации

Настройте Self-Defined Guard для устранения проблем с сетевыми атаками в особых сценариях.

11.4.7.2. Примечания

- Для команды, настроенной как в режиме конфигурации Self-Defined Guard, так и в режиме конфигурации интерфейса, конфигурация в режиме конфигурации интерфейса имеет приоритет над конфигурацией, настроенной в режиме конфигурации Self-Defined Guard.
- Self-Defined Guard имеет приоритет над основными Guard’ами.

11.4.7.3. Шаги настройки

Настройка Guard Name

- (Обязательно) Настройте имя Self-Defined Guard, чтобы создать Self-Defined Guard.
- Имя должно быть уникальным, а поля соответствия и значения должны отличаться от полей ARP, ICMP, DHCP, IP и DHCPv6 Guard’ов. Если параметры, которые вы хотите настроить, уже существуют, отображается сообщение, указывающее на ошибку конфигурации.

Настройка полей соответствия

- Обязательный.

- Самоопределяемые пакеты классифицируются на основе следующих полей: etype (тип канального уровня Ethernet), smac (MAC-адрес источника), dmac (MAC-адрес получателя), protocol (номер протокола IPv4/IPv6), sip (IPv4/IPv6-адрес источника), dip (IPv4/IPv6-адрес назначения), sport (порт исходного транспортного уровня) и dport (порт транспортного уровня назначения).
- **protocol** действителен, только если значением **etype** является **ipv4** или **ipv6**. **src-ip** и **dst-ip** допустимы, только если значением **etype** является **ipv4**. **src-ipv6** и **dst-ipv6** допустимы, только если значением **etype** является **ipv6**. **src-port** и **dst-port** допустимы, только если значение **protocol** равно **tcp** или **udp**.
- Если поля совпадения (**match** fields) и значения Self-Defined Guard полностью такие же, как у существующей Guard, система печатает журнал «%ERROR: the match type and value are the same with define name (name of an existing guard).", чтобы уведомить администратора об ошибке конфигурации.
- Если **protocol** настроен, но в политике сопоставления (**match** policy) **etype** указан как IPv4 или IPv6, система печатает журнал «%ERROR: protocol is valid only when etype is IPv4(0x0800) or IPv6(0x86dd).».
- Если **src-ip** и **dst-ip** настроены, но **etype** не является IPv4 в политике соответствия, система печатает журнал «%ERROR: IP address is valid only when etype is IPv4(0x0800).».
- Если **src-ipv6** и **dst-ipv6** настроены, но **etype** не является IPv6 в политике соответствия, система печатает журнал «%ERROR: IPv6 address is valid only when etype is IPv6(0x86dd).».
- Если **src-port** и **dst-port** настроены, но **protocol** не является TCP или UDP в политике сопоставления, система печатает журнал «%ERROR: Port is valid only when protocol is TCP(6) or UDP(17).».
- В следующей таблице перечислены политики защиты, соответствующие некоторым распространенным сетевым протоколам. Ограничения скорости и пороги атак, перечисленные ниже, могут соответствовать требованиям в большинстве сетевых сценариев и приведены только для справки. Вы можете настроить допустимые ограничения скорости и пороги атаки на основе реальных сценариев.

protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
RIP	etype 0x0800 protocol 17 dst-port 520	rate-limit 100 attatch-threshold 150	Не применимо к этой политике	rate-limit 300 attatch-threshold 500
RIPng	etype 0x86dd protocol 17 dst-port 521	rate-limit 100 attatch-threshold 150	Не применимо к этой политике	rate-limit 300 attatch-threshold 500
BGP	etype 0x0800 protocol 6 dst-port 179	rate-limit 1000 attatch-threshold 1200	Не применимо к этой политике	rate-limit 2000 attatch-threshold 3000

protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
BPDU	dst-mac 08c6.b300.0000	Не применимо к этой политике	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
RERP	dst-mac 08c6.b300.0001	Не применимо к этой политике	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
REUP	dst-mac 08c6.b300.0007	Не применимо к этой политике	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
BGP	etype 0x0800 protocol 6 dst-port 179	Не применимо к этой политике	Не применимо к этой политике	Не применимо к этой политике
OSPFv2	etype 0x0800 protocol 89	rate-limit 800 attatch-threshold 1200	Не применимо к этой политике	rate-limit 2000 attatch-threshold 3000
OSPFv3	etype 0x86dd protocol 89	rate-limit 800 attatch-threshold 1200	Не применимо к этой политике	rate-limit 2000 attatch-threshold 3000
VRRP	etype 0x0800 protocol 112	rate-limit 64 attatch-threshold 100	Не применимо к этой политике	rate-limit 1024 attatch-threshold 1024
IPv6 VRRP	etype 0x86dd protocol 112	rate-limit 64 attatch-threshold 100	Не применимо к этой политике	rate-limit 1024 attatch-threshold 1024
SNMP	etype 0x0800 protocol 17 dst-port 161	rate-limit 1000 attatch-threshold 1200	Не применимо к этой политике	rate-limit 2000 attatch-threshold 3000
RSVP	etype 0x0800 protocol 46	rate-limit 800 attatch-threshold 1200	Не применимо к этой политике	rate-limit 1200 attatch-threshold 1500

protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
LDP (UDP hello)	etype 0x0800 protocol 17 dst-port 646	rate-limit 10 attatch-threshold 15	Не применимо к этой политике	rate-limit 100 attatch-threshold 150

- Чтобы содержать как можно больше существующих типов протоколов и облегчить расширение новых типов протоколов, self-defined guard позволяют хостам свободно комбинировать поля типов пакетов. Если конфигурация не подходит, сеть может выйти из строя. Поэтому сетевой администратор должен хорошо знать сетевые протоколы. В качестве справки в следующей таблице перечислены допустимые конфигурации известных в настоящее время протоколов для общих политик self-defined guard. Для других протоколов, не перечисленных в таблице, настраивайте их с осторожностью.

Настройка глобального ограничения скорости и порога атаки

- (Обязательно) Если эти параметры не настроены, self-defined guard нельзя включить.
- Вы должны настроить одно из полей **per-src-ip**, **per-src-mac** и **per-port**. В противном случае политика не может вступить в силу.
- **per-src-ip** действителен, только если **etype** имеет значение IPv4 или IPv6.
- Ограничение скорости, настроенное на основе исходного MAC-адреса, идентификатора VLAN и порта, имеет приоритет над ограничением, настроенным на основе исходного IP-адреса, идентификатора VLAN и порта.
- Политика идентификации хоста на основе портов self-defined guard должна быть согласована с глобальной политикой идентификации хостов на основе портов.
- Если политика **per-src-ip** настроена не глобально, а настроена для порта, система печатает журнал «%ERROR: name (name of a self-defined guard) has not per-src-ip policy.», чтобы уведомить администратора об ошибке конфигурации.
- Если политика **per-src-mac** настроена не глобально, а настроена для порта, система печатает журнал «%ERROR: name (name of a self-defined guard) has not per-src-mac policy.», чтобы уведомить администратора об ошибке конфигурации.
- Если память не может быть выделена обнаруженным злоумышленникам, система печатает журнал «%NFPP_DEFINE_GUARD-4-NO_MEMORY: Failed to allocate memory.», чтобы уведомить администратора.
- Если настроенное ограничение скорости больше порога атаки, система печатает журнал «%ERROR: rate limit is higher than attack threshold 500pps.», чтобы уведомить администратора.
- Если настроенный порог атаки меньше ограничения скорости, система печатает журнал «%ERROR: attack threshold is smaller than rate limit 300pps.», чтобы уведомить администратора.

Настройка периода глобального мониторинга

- (Обязательно) Период мониторинга по умолчанию составляет 600 секунд.
- Если период изоляции настроен, он напрямую используется в качестве периода мониторинга, и настроенный период мониторинга теряет силу.
- Период мониторинга можно настроить в режиме self-defined guard.

- Если период изоляции равен 0, система выполняет программный мониторинг обнаруженных злоумышленников. Период тайм-аута является периодом мониторинга. Если во время мониторинга программного обеспечения для периода изоляции установлено ненулевое значение, система автоматически выполняет аппаратную изоляцию от контролируемых злоумышленников и устанавливает период ожидания в качестве периода мониторинга. Период мониторинга действителен, только если период изоляции равен 0.
- Если период изоляции изменен на 0, злоумышленники, использующие соответствующий порт, удаляются, а не отслеживаются.

Настройка максимального количества отслеживаемых хостов

- (Обязательно) По умолчанию максимальное количество отслеживаемых хостов составляет 20 000.
- Разумно установите максимальное количество отслеживаемых хостов. По мере увеличения количества отслеживаемых хостов используется больше ресурсов ЦП.
- Максимальное количество контролируемых хостов можно настроить в режиме self-defined guard.
- Если количество отслеживаемых хостов достигает 20 000 (значение по умолчанию), а администратор устанавливает максимальное число ниже 20 000, система не удаляет отслеживаемые хосты, а печатает журнал «%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts.». Эта информация уведомляет администратора о том, что конфигурация не вступает в силу и что некоторые отслеживаемые хосты необходимо удалить.
- Если таблица отслеживаемых хостов заполнена, система печатает журнал «% NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 20000 monitored hosts.», чтобы уведомить администратора.

Настройка доверенных хостов

- (Опционально) По умолчанию доверенный хост не настроен.
- Вы можете настроить до 500 доверенных IP-адресов или MAC-адресов для self-defined guard.
- Доверенные хосты могут быть настроены в режиме self-defined guard.
- Если вы не хотите отслеживать хост, вы можете запустить следующие команды, чтобы доверять хосту. Этот доверенный хост может отправлять ICMP-пакеты на ЦП без каких-либо ограничений скорости или предупреждающих сообщений. Маску можно настроить таким образом, чтобы ни один хост в одном сегменте сети не отслеживался.
- Перед настройкой доверенных хостов необходимо настроить тип соответствия. Если тип пакета — IPv4 в политике сопоставления, вам не разрешено настраивать доверенные адреса IPv6. Если тип пакета — IPv6 в политике сопоставления, вам не разрешено настраивать доверенные адреса IPv4.
- Если тип соответствия не настроен, система печатает журнал «%ERROR: Please configure match rule first.».
- Если добавлен доверенный хост IPv4, но **etype** не является IPv4 в политике сопоставления, система распечатает журнал «%ERROR: Match type can’t support IPv4 trusted host.».

- Если добавлен доверенный хост IPv6, но **etype** не является IPv6 в политике сопоставления, система печатает журнал «%ERROR: Match type can’t support IPv6 trusted host.».
- Если таблица доверенных хостов заполнена, система печатает журнал «%ERROR: Attempt to exceed limit of 500 trusted hosts.», чтобы уведомить администратора.
- Если в таблице отслеживаемых хостов существует какая-либо запись, соответствующая доверенному хосту (IP-адреса совпадают), система автоматически удаляет эту запись.
- Если доверенный хост не может быть удален, система печатает журнал «%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0.», чтобы уведомить администратора.
- Если хосту нельзя доверять, система печатает журнал «%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0.», чтобы уведомить администратора.
- Если хост, которому можно доверять, уже существует, система печатает журнал «%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured.», чтобы уведомить администратора.
- Если хост, который необходимо удалить из доверенной таблицы, не существует, система печатает журнал «%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found.», чтобы уведомить администратора.
- Если память не может быть выделена доверенному узлу, система печатает журнал «%ERROR: Failed to allocate memory.», чтобы уведомить администратора.

Включение Self-Defined Guard

- Обязательный.
- Вы должны настроить по крайней мере одну политику между политикой Self-Defined Guard на основе хоста и политикой Self-Defined Guard на основе порта. В противном случае Self-Defined Guard не может быть включена.
- Если Self-Defined Guard отключена, система автоматически очищает отслеживаемые хосты.
- Self-Defined Guard можно настроить в режиме Self-Defined Guard или в режиме настройки интерфейса.
- Если политика Self-Defined Guard настроена не полностью, Self-Defined Guard не может быть включена, и отображается запрос на уведомление хостов об отсутствующих конфигурациях политики.
- Если имя Self-Defined Guard не существует, система печатает журнал «%ERROR: The name is not exist.».
- Если тип соответствия не настроен для Self-Defined Guard, система печатает журнал «%ERROR: name (name of the self-defined guard) doesn't match any type.».
- Если политика для Self-Defined Guard не настроена, система печатает журнал «%ERROR: name (name of the self-defined guard) doesn't specify any policy.».

11.4.7.4. Проверка

Когда хост в сети отправляет пакеты на коммутатор, настроенный с Self-Defined Guard NFPP, проверьте, могут ли эти пакеты быть отправлены на ЦП.

- Если скорость пакетов от ненадежного хоста превышает порог атаки, отображается журнал атак.

- Если для злоумышленника создается изолированная запись, отображается журнал изоляции.

11.4.7.5. Связанные команды

Настройка имени Self-Defined Guard

Команда	**define** *name*
Описание параметров	*name*: указывает имя Self-Defined Guard
Командный режим	Режим конфигурации NFPP

Настройка полей совпадения Self-Defined Guard

Команда	**match** [**etype** *type*] [**src-mac** *smac* [**src-mac-mask** *smac_mask*]] [**dst-mac** *dmac* [**dst-mac-mask** *dst_mask*]] [**protocol** *protocol*] [**src-ip** *sip* [**src-ip-mask** *sip-mask*]] [**src-ipv6** *sipv6* [**src-ipv6-masklen** *sipv6-masklen*]] [**dst-ip** *dip*[**dst-ip-mask** *dip-mask*]] [**dst-ipv6** *dipv6* [**dst-ipv6-masklen** *dipv6-masklen*]][**src-port** *sport*] [**dst-port** *dport*]
Описание параметров	*type*: указывает тип пакетов канального уровня Ethernet. *smac*: указывает MAC-адрес источника. *smac_mask*: указывает маску исходного MAC-адреса. *dmac*: указывает MAC-адрес назначения. *dst_mask*: указывает маску MAC-адреса назначения. *protocol*: указывает номер протокола пакетов IPv4/IPv6. *sip*: указывает исходный адрес IPv4. *sip-mask*: указывает маску исходного IPv4-адреса. *sipv6*: указывает исходный IPv6-адрес. *sipv6-masklen*: указывает длину маски исходного IPv6-адреса. *dip*: указывает IPv4-адрес назначения. *dip-mask*: указывает маску IPv4-адреса назначения. *dipv6*: указывает IPv6-адрес назначения. *dipv6-masklen*: указывает длину маски IPv6-адреса назначения. *sport*: указывает идентификатор исходного порта транспортного уровня. *dport*: указывает идентификатор целевого порта транспортного уровня
Командный режим	Режим конфигурации Self-Defined Guard

Руководство по использованию	Создайте новую Self-Defined Guard и укажите поля пакета, соответствующие этой защите

Настройка глобального ограничения скорости и порога атаки Self-Defined Guard

Команда	**global-policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Описание параметров	**per-src-ip**: собирает статистику скорости для идентификации хоста на основе исходного IP-адреса, идентификатора VLAN и порта. **per-src-mac**: собирает статистику скорости для идентификации хоста на основе исходного MAC-адреса, идентификатора VLAN и порта. **per-port**: собирает статистику скорости на основе каждого порта приема пакетов. *rate-limit-pps*: указывает ограничение скорости. *attack-threshold-pps*: указывает порог атаки
Командный режим	Режим конфигурации Self-Defined Guard
Руководство по использованию	Перед созданием типа Self-Defined Guard необходимо указать правила классификации статистики скорости для этого типа, а именно: идентификацию хоста на основе исходного IP-адреса, идентификацию хоста на основе MAC-адреса источника, самоопределяемую статистику скорости передачи пакетов на основе хоста или статистики скорости на основе порта и указать ограничения скорости и пороги атаки для указанных правил

Настройка периода глобального мониторинга Self-Defined Guard

Команда	**monitor-period** *seconds*
Описание параметров	*seconds*: указывает период мониторинга в секундах. Значение колеблется от 180 до 86 400
Командный режим	Режим конфигурации Self-Defined Guard

Настройка максимального количества контролируемых хостов Self-Defined Guard

Команда	**monitored-host-limit** *number*
Описание параметров	*number*: указывает максимальное количество отслеживаемых хостов в диапазоне от 1 до 4 294 967 295

Командный режим	Режим конфигурации Self-Defined Guard

Настройка доверенных хостов Self-Defined Guard

Команда	**trusted-host** {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}
Описание параметров	*mac*: указывает MAC-адрес. *mac_mask*: указывает маску MAC-адреса. *ip*: указывает IP-адрес. *mask*: указывает маску IP-адреса. *IPv6/prefixlen*: указывает адрес IPv6 и длину его маски. **all**: используется с **no** для удаления всех доверенных хостов
Командный режим	Режим конфигурации Self-Defined Guard

Глобальное включение Self-Defined Guard

Команда	**define** *name* **enable**
Описание параметров	*name*: указывает имя Self-Defined Guard
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Конфигурация вступает в силу только после того, как вы настроите match, rate-count, rate-limit и attack-threshold. В противном случае конфигурация не работает

Включение Self-Defined Guard на интерфейсе

Команда	**nfpp define** *name* **enable**
Описание параметров	*name*: указывает имя Self-Defined Guard
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Самоопределяемое (Self-Defined) имя должно существовать. Конфигурация вступает в силу только после того, как вы настроите match, rate-count, rate-limit и attack-threshold. В противном случае конфигурация не работает

Настройка ограничения скорости и порога атаки Self-Defined Guard на интерфейсе

Команда	**nfpp define** *name* **policy** {**per-src-ip** | **per-src-mac**| **per-port**} *rate-limit-pps attack-threshold-pps*
Описание параметров	*name*: указывает имя Self-Defined Guard. **per-src-ip**: настраивает ограничение скорости и порог атаки для каждого исходного IP-адреса. **per-src-mac**: настраивает ограничение скорости и порог атаки для каждого MAC-адреса источника. **per-port**: настраивает ограничение скорости и порог атаки для каждого порта. *rate-limit-pps*: указывает ограничение скорости в диапазоне от 1 до 19999. *attack-threshold-pps*: указывает порог атаки в диапазоне от 1 до 19 999
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Порог атаки должен быть равен или превышать предел скорости

11.4.7.6. Пример конфигурации

Защита ЦП на основе Self-Defined Guard

Сценарий	Базовые guard'ы не могут защитить систему от RIP-атак
Шаги настройки	Настройте Self-Defined Guard с ключевыми полями, соответствующими пакетам RIP. Настройте ограничение скорости. Настройте доверенные хосты
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#define rip QTECH (config-nfpp-define)#match etype 0x0800 protocol 17 dst-port 520 QTECH (config-nfpp-define)#global-policy per-src-ip 100 150 QTECH (config-nfpp-define)#trusted-host 192.168.201.46 255.255.255.255 QTECH (config-nfpp-define)#exit QTECH (config-nfpp)#define rip enable

Проверка	Запустите команду **show nfpp define summary rip**, чтобы отобразить конфигурацию
	Define rip summary: match etype 0x800 protocol 17 dst-port 520 Maximum count of monitored hosts: 1000 Monitor period:600s (Format of column Rate-limit and Attack-threshold is per-src-ip/per-srcmac/per-port.) Interface Status Rate-limit Attack-threshold Global Enable 100/-/- 150/-/-
	Запустите команду show nfpp define trusted-host rip, чтобы отобразить доверенные хосты
	Define rip: IP trusted host number is 1: IP address IP mask ---------- ------- 192.168.201.46 255.255.255.255 Total: 1 record(s)Global Enable 180 100/-/- 150/-/-
	Запустите команду **show nfpp define hosts rip**, чтобы отобразить отслеживаемые хосты
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address remain-time(s) ---- --------- ---------- -------------- 1 Gi0/5 192.168.201.47 160 Total: 1 host

11.4.8. Настройка централизованного распределения полосы пропускания

11.4.8.1. Эффект конфигурации

Настройте централизованное распределения пропускной способности, чтобы пакеты управления и протокола обрабатывались в первую очередь, когда сеть занята.

11.4.8.2. Примечания

Должно быть выполнено следующее условие: допустимый процентный диапазон типа пакетов ≤ 100 % — процент суммы двух других типов.

11.4.8.3. Шаги настройки

Настройка максимальной пропускной способности указанных пакетов

(Обязательно) Пакеты управления, маршрутизации и протокола используют одну и ту же полосу пропускания по умолчанию.

Настройка максимального процента указанных пакетов в очереди

(Обязательно) По умолчанию пакеты управления занимают 30 % пропускной способности, пакеты маршрута занимают 25 %, а пакеты протокола занимают 45 %.

11.4.8.4. Проверка

Отправьте большое количество протокольных пакетов, таких как пакеты OSPF, на коммутатор, что приводит к высокой загрузке ЦП.

Когда хост пингует коммутатор, проверка связи должна быть успешной, и ни один пакет не будет потерян.

11.4.8.5. Связанные команды

Настройка максимальной пропускной способности указанных пакетов

Команда	**cpu-protect sub-interface** { **manage** | **protocol** | **route**} **pps** *pps_value*
Описание параметров	*pps_value*: указывает ограничение скорости в диапазоне от 1 до 100000
Командный режим	Режим глобальной конфигурации

Настройка максимального процента указанных пакетов в очереди

Команда	**cpu-protect sub-interface** { **manage** | **protocol** | **route**} **percent** *percent_value*
Описание параметров	*percent_value*: указывает процент пакетов определенного типа в очереди в диапазоне от 1 до 100
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Должно быть выполнено следующее условие: допустимый процентный диапазон типа пакетов ≤ 100% — процент суммы двух других типов

11.4.8.6. Пример конфигурации

Приоритизация пакетов, отправляемых на ЦП посредством централизованного распределения пропускной способности

Сценарий	В сети существуют различные типы массовых пакетов, которые относятся к разным централизованным типам

Шаги настройки	Настройте максимальную пропускную способность указанных пакетов. Настройте максимальный процент указанных пакетов в очереди
	QTECH# configure terminal QTECH(config)# cpu-protect sub-interface manage pps 5000 QTECH(config)# cpu-protect sub-interface manage percent 25

11.4.9. Настройка ведения журнала NFPP

11.4.9.1. Эффект конфигурации

NFPP получает журнал из выделенного буфера журнала с определенной скоростью, генерирует системное сообщение и очищает этот журнал из выделенного буфера журнала.

11.4.9.2. Примечания

Журналы непрерывно печатаются в буфере журналов, даже если атаки прекратились.

11.4.9.3. Шаги настройки

Настройка размера буфера журнала

Обязательный.

Если буфер журнала заполнен, новые журналы заменяют старые.

Если буфер журнала переполняется, последующие журналы заменяют предыдущие журналы, и в буфере журнала отображается запись со всеми атрибутами, отмеченными дефисом (-). Администратору необходимо увеличить размер буфера журнала или скорость генерации системных сообщений.

Настройка скорости буферизации журнала

Обязательный.

Скорость буферизации журнала зависит от двух параметров: периода времени и количества системных сообщений, сгенерированных за этот период времени.

Если оба предыдущих параметра установлены на 0, системные сообщения немедленно генерируются для журналов, но не сохраняются в буфере журналов.

Включение фильтрации журналов

(Опционально) Фильтрация журналов по умолчанию отключена.

Журналы можно фильтровать на основе интерфейса или VLAN.

Если фильтрация журналов включена, журналы, не соответствующие правилу фильтрации, отбрасываются.

Включение печати журнала

(Обязательно) Журналы по умолчанию хранятся в буфере.

Если вы хотите отслеживать атаки в режиме реального времени, вы можете настроить печать журналов на экране для экспорта информации журнала в режиме реального времени.

11.4.9.4. Проверка

Проверьте, действует ли конфигурация на основе конфигурации журнала, а также количества и интервала распечатываемых журналов.

11.4.9.5. Связанные команды

Настройка размера буфера журнала

Команда	**log-buffer entries** *number*
Описание параметров	*number*: указывает размер буфера в единицах количества журналов в диапазоне от 0 до 1024
Командный режим	Режим конфигурации NFPP

Настройка скорости буферизации журнала

Команда	**log-buffer logs** *number_of_message* **interval** *length_in_seconds*
Описание параметров	*number_of_message*: диапазон от 0 до 1024. Значение 0 указывает, что все журналы записываются в буфер журналов и системное сообщение не генерируется. *length_in_seconds*: диапазон от 0 до 86 400 (1 день). Значение 0 указывает, что журналы не записываются в буфер журналов, но системные сообщения генерируются мгновенно. Это также относится к *number_of_message* и *length_in_seconds*. *number_of_message/length_in_second* указывает скорость генерации системных сообщений
Командный режим	Режим конфигурации NFPP

Настройка фильтрации журналов на основе VLAN

Команда	**logging vlan** *vlan-range*
Описание параметров	*vlan-range*: записывает журналы в указанном диапазоне VLAN. Например, формат значения 1-3,5
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Запустите эту команду, чтобы отфильтровать журналы, чтобы записывались только журналы в указанном диапазоне VLAN. Между фильтрацией журналов на основе интерфейса и фильтрацией журналов на основе VLAN, если выполняется какое-либо правило, журналы записываются в буфер журналов

Настройка фильтрации журналов на основе интерфейса

Команда	**logging interface** *interface-id*
Описание параметров	*interface-id*: записывает журналы указанного интерфейса
Командный режим	Режим конфигурации NFPP
Руководство по использованию	Запустите эту команду, чтобы отфильтровать журналы, чтобы только журналы указанного интерфейса записывались. Между фильтрацией журналов на основе интерфейса и фильтрацией журналов на основе VLAN, если выполняется какое-либо правило, журналы записываются в буфер журналов

Включение печати журнала

Команда	**log-buffer enable**
Командный режим	Режим конфигурации NFPP

11.4.9.6. Пример конфигурации

Настройка ведения журнала NFPP

Сценарий	Если злоумышленников слишком много, печать журнала повлияет на использование пользовательских интерфейсов, что требует ограничения
Шаги настройки	• Настройте размер буфера журнала. • Настройте скорость буферизации журнала. • Настройте фильтрацию журналов на основе VLAN
	QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#log-buffer entries 1024 QTECH (config-nfpp)#log-buffer logs 3 interval 5 QTECH (config-nfpp)#logging interface vlan 1
Проверка	Запустите команду **show nfpp log summary**, чтобы отобразить конфигурацию
	Total log buffer size : 1024 Syslog rate : 3 entry per 5 seconds Logging:

	VLAN 1
	Запустите команду **show nfpp log buffer**, чтобы отобразить журналы в буфере журналов
	Protocol VLAN Interface IP address MAC address Reason Timestamp -------- ---- --------- ---------- ----------- ------ --------- ARP 1 Gi0/5 192.168.206.2 08c6.b3c2.4609 SCAN 2013-5-1 5:4:24

11.5. Мониторинг

11.5.1. Очистка

Описание	Команда
Очищает таблицу сканирования ARP Guard	**clear nfpp arp-guard scan**
Очищает хосты, отслеживаемые ARP Guard	**clear nfpp arp-guard hosts**
Очищает хосты, отслеживаемые IP Guard	**clear nfpp ip-guard hosts**
Очищает хосты, отслеживаемые ND Guard	**clear nfpp nd-guard hosts**
Очищает хосты, отслеживаемые ICMP Guard	**clear nfpp icmp-guard hosts**
Очищает хосты, отслеживаемые DHCP Guard	**clear nfpp dhcp-guard hosts**
Очищает хосты, отслеживаемые DHCPv6 Guard	**clear nfpp dhcpv6-guard hosts**
Очищает хосты, отслеживаемые Self-Defined Guard	**clear nfpp define** *name* **hosts**
Очищает журналы NFPP	**clear nfpp log**

11.5.2. Отображение

Описание	Команда
Отображает конфигурацию ARP Guard	**show nfpp arp-guard summary**
Отображает хосты, отслеживаемые ARP Guard	**show nfpp arp-guard hosts**

Описание	Команда
Отображает таблицу сканирования ARP Guard	**show nfpp arp-guard scan**
Отображает конфигурацию IP Guard	**show nfpp ip-guard summary**
Отображает хосты, контролируемые IP Guard	**show nfpp ip-guard hosts**
Отображает таблицу сканирования IP Guard	**show nfpp ip-guard trusted-host**
Отображает конфигурацию ICMP Guard	**show nfpp icmp-guard summary**
Отображает хосты, контролируемые ICMP Guard	**show nfpp icmp-guard hosts**
Отображает таблицу сканирования ICMP Guard	**show nfpp icmp-guard trusted-host**
Отображает конфигурацию DHCP Guard	**show nfpp dhcp-guard summary**
Отображает хосты, контролируемые DHCP Guard	**show nfpp dhcp-guard hosts**
Отображает конфигурацию DHCPv6 Guard	**show nfpp dhcpv6-guard summary**
Отображает хосты, отслеживаемые DHCPv6 Guard	**show nfpp dhcpv6-guard hosts**
Отображает конфигурацию ND Guard	**show nfpp nd-guard summary**
Отображает конфигурацию Self-Defined Guard	**show nfpp define summary [***name***]**
Отображает отслеживаемые хосты	**show nfpp define hosts** *name*
Отображает доверенные хосты	**show nfpp define trusted-host** *name*
Отображает журналы NFPP	**show nfpp log summary**
Отображает буфер журнала NFPP	**show nfpp log buffer [statistics]**

12. ОБЩАЯ ИНФОРМАЦИЯ

12.1. 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.

12.2. 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

12.3. Электронная версия документа

Дата публикации 10.03.2025

https://files.qtech.ru/upload/switchers/QSW-4700/QSW-4700_security_config_guide.pdf