Эфрос-сканер

Назначение

Сканирование маршрутизаторов и МСЭ Cisco на основе сценариев и заданий, создание базы данных с описанием команд, их параметров и уровней привилегий.

© ООО «Газинформсервис»

Эфрос-сканер

Автоматизация процесса получения списка команд ОС Cisco IOS

Сканер взаимодействует со справочной подсистемой ОС Cisco IOS (Cisco Pix) и на основе сценария осуществляет формирование цепочек вариантов допустимых для выполнения на маршрутизаторе команд для пользователя с заданным уровнем привилегий.

© ООО «Газинформсервис»

Эфрос-сканер

Слияние

Дополнительно в рамках оболочки сканера реализована поддержка слияния команд, выявленных на различных уровнях привилегий. Необходимость слияния связана с тем, что в состав команд пользователя с уровнем привилегий **K** входят команды уровней привилегий и меньше **K**.

© ООО «Газинформсервис»

Эфрос-сканер

Автоматизация процесса получения списка команд ОС Cisco IOS

Результатом работы сканера является набор файлов, содержащих описания возможных вариантов цепочек операндов команд ОС Cisco IOS для соответствующего режима интерпретатора командной строки.

© ООО «Газинформсервис»

Пример работы системы

Эфрос-сканер

Задача: получить список команд маршрутизатора в режиме EXEC

© ООО «Газинформсервис»

План работы

- Создание нового маршрутизатора
- Задание параметров сканирования
- Задание параметров замены
- Задание параметров дополнения
- Задание параметров сканирования для режима EXEC с различными уровнями привилегий
- Сканирование
- Задание параметров слияния
- Слияние
- Просмотр результатов

© ООО «Газинформсервис»

Создание нового маршрутизатора

Имя проекта.
Папка с этим именем появится в директории
../<место установки>/Эфрос-сканер/Routers/

IP-адрес маршрутизатора

Порт для связи по протоколу Telnet

© ООО «Газинформсервис»

Задание параметров сканирования

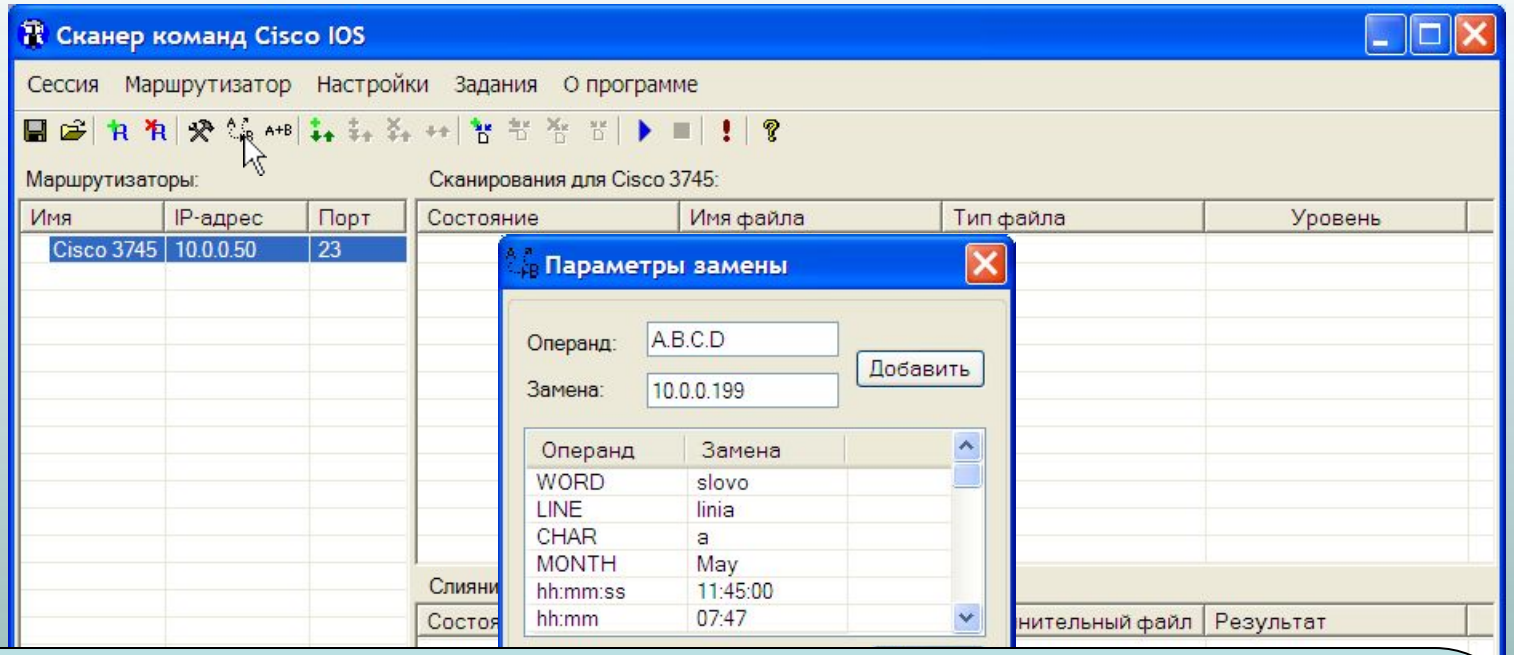
Сетевое имя маршрутизатора заданное командой
`Router(config)#hostname c3745`

Количество сканируемых подкоманд

Запись протокола сканирования в файл
../<место установки>/Эфрос-сканер/Routers/<Имя проекта>/Temp/report.log

© ООО «Газинформсервис»

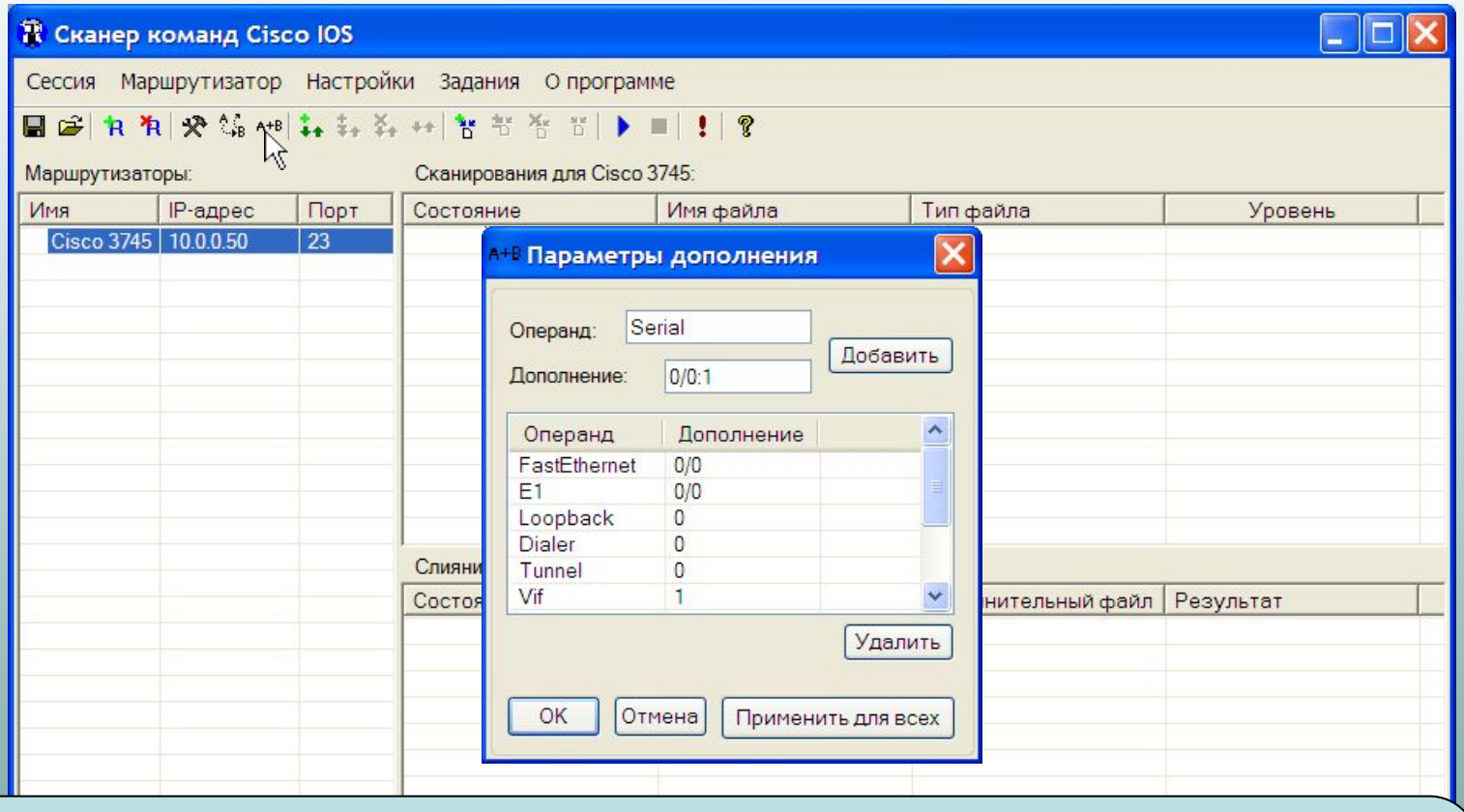
Задание параметров замены



Сканирование команд осуществляется с использованием справочной службы команд Cisco IOS. При обращении к справке команды в ряде случаев требуется задание конкретных значений операндов. Для корректной работы сканера команд необходимо указать соответствие между обобщенным обозначением операнда команды и применяемым конкретным значением. Например, для того, чтобы отсканировать все операнды команды ***clock set*** необходимо указать для ***hh:mm:ss*** вариант конкретного значения, в частности ***11:45:00***.

Список замен зависит от конкретной модели маршрутизатора и типа операционной системы.

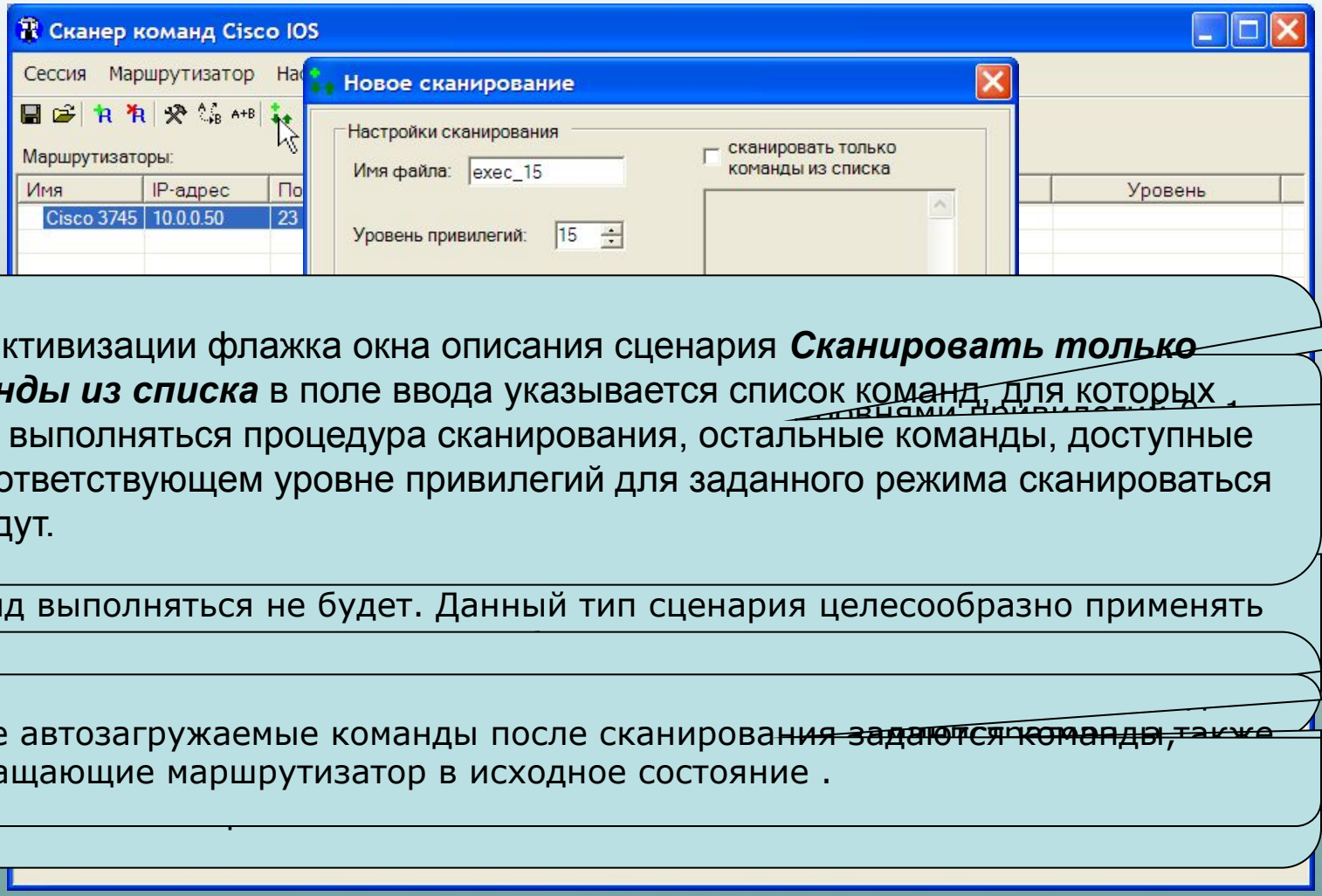
Задание параметров дополнения



Доступность ряда команд Cisco IOS зависит от конфигурации, в частности от наличия и числа физических и логических интерфейсов. Для обеспечения корректного сканирования таких команд необходимо указать конкретные значения сконфигурированнных интерфейсов.

© ООО «Газинформсервис»

Задание параметров сканирования



При активизации флажка окна описания сценария ***Сканировать только команды из списка*** в поле ввода указывается список команд, для которых будет выполняться процедура сканирования, остальные команды, доступные на соответствующем уровне привилегий для заданного режима сканироваться не будут.

команд выполняться не будет. Данный тип сценария целесообразно применять

В поле автозагружаемые команды после сканирования задаются команды, также возвращающие маршрутизатор в исходное состояние .

© ООО «Газинформсервис»

Задание параметров сканирования

Сканер команд Cisco IOS

Сессия Маршрутизатор Нас

Маршрутизаторы:

Имя	IP-адрес	По
Cisco 3745	10.0.0.50	23

Уровень

Результат

Новое сканирование

Настройки сканирования

Имя файла: exec_0

Уровень привилегий: 0

временный файл (не помещать в результат)

Выполнять сканирование

сканировать только команды из списка

Автозагружаемые команды

До сканирования:

user
password
enable
enable password

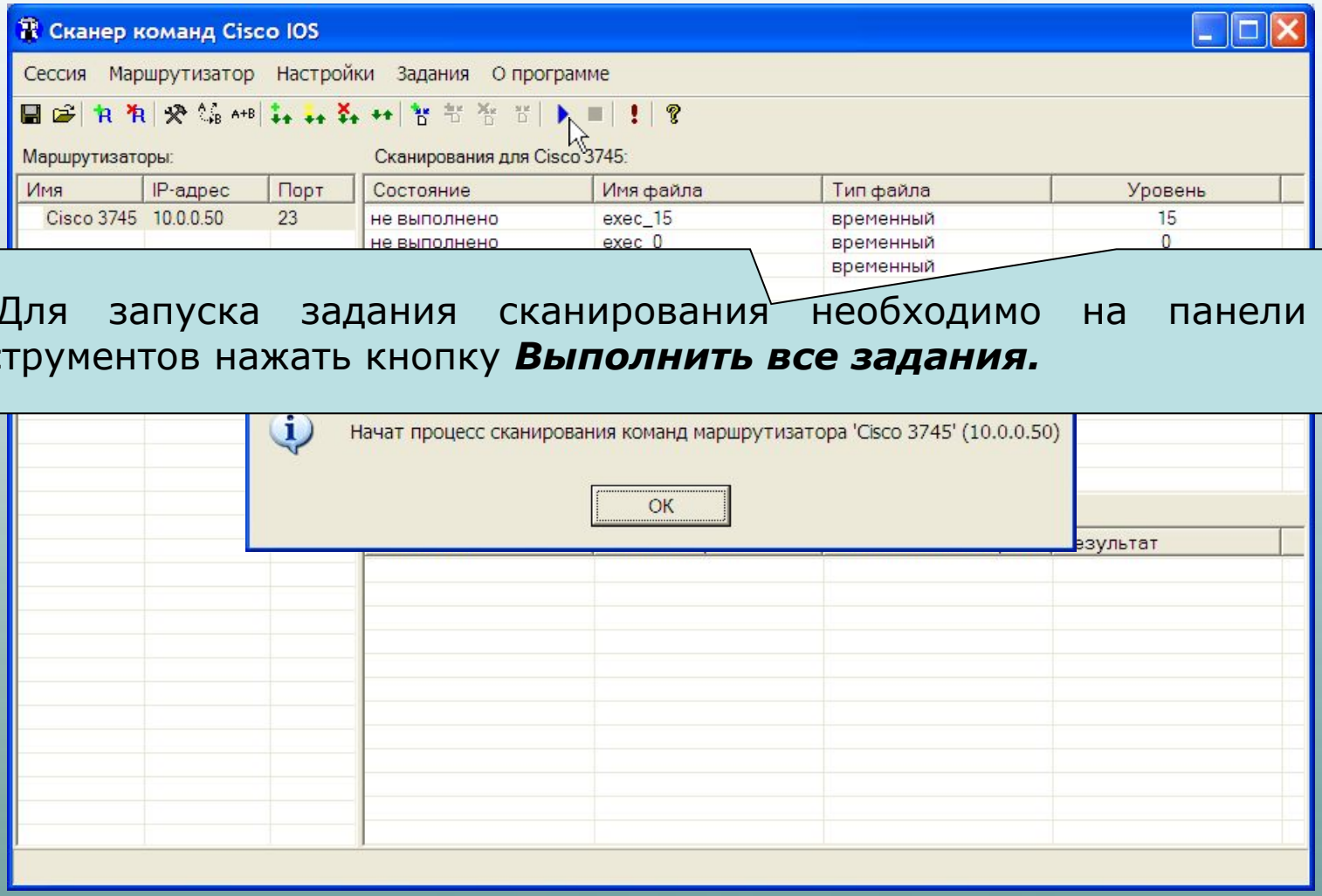
disable 0

После сканирования:

Параметры сканирования необходимо задать для всех уровней привилегий, доступных на маршрутизаторе

© ООО «Газинформсервис»

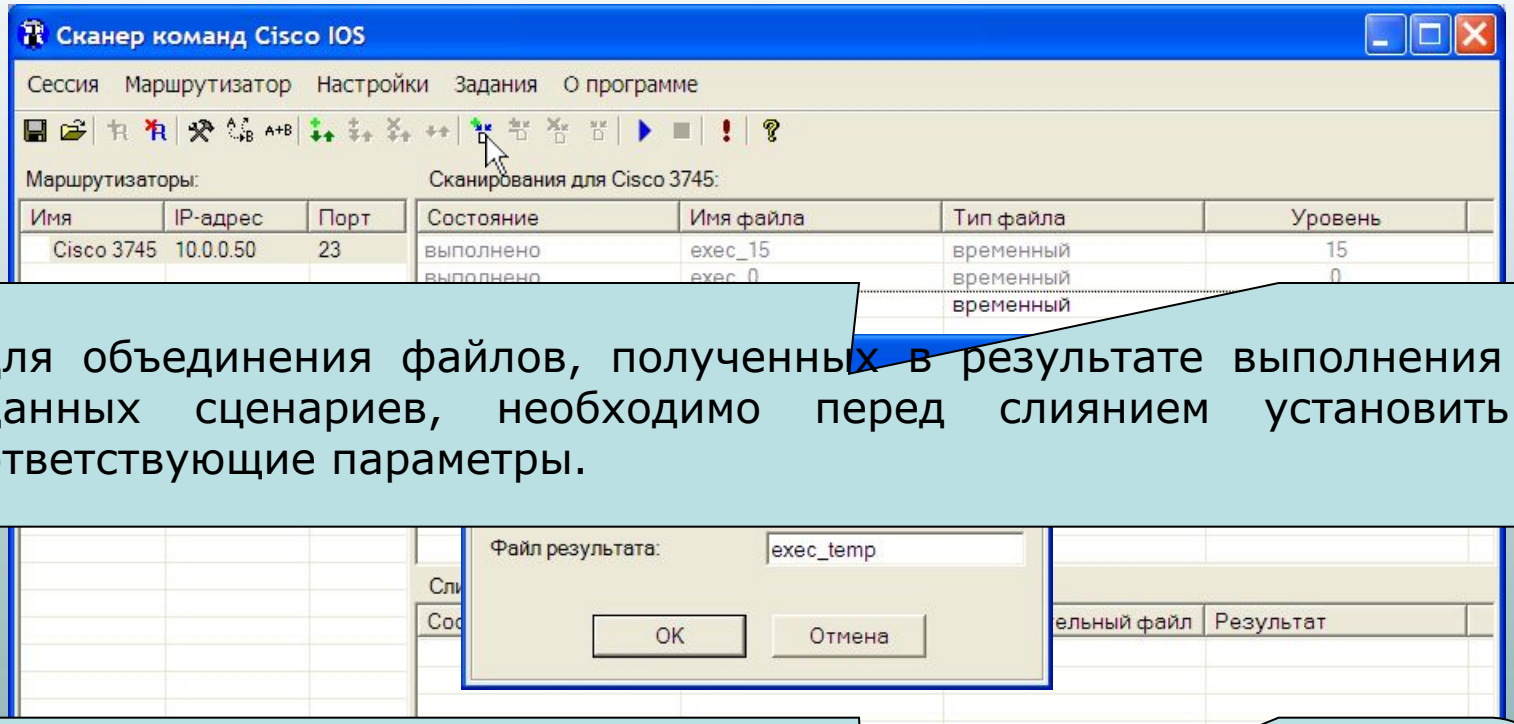
Начало процесса сканирования



Для запуска задания сканирования необходимо на панели инструментов нажать кнопку ***Выполнить все задания.***

© ООО «Газинформсервис»

Задание параметров слияния

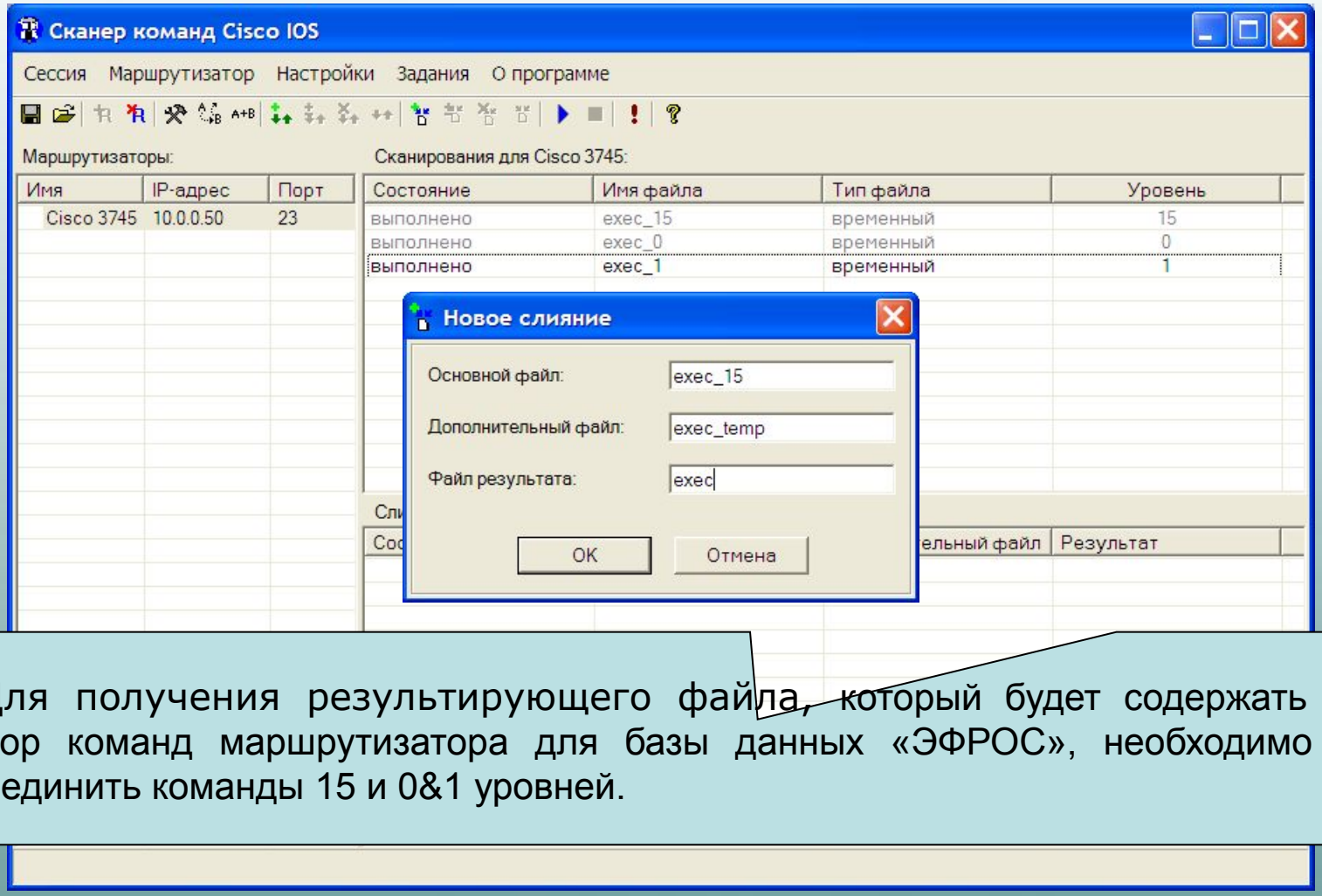


Для объединения файлов, полученных в результате выполнения заданных сценариев, необходимо перед слиянием установить соответствующие параметры.

В поле «Основной файл» задается имя основного файла – файла с командами **более высокого** уровня привилегий, в поле «Дополнительный файл» указывается имя дополнительного файла для слияния и в поле «Файл результата» — имя результирующего файла, в данном случае это временный файл с командами 0 и 1 уровня

© ООО «Газинформсервис»

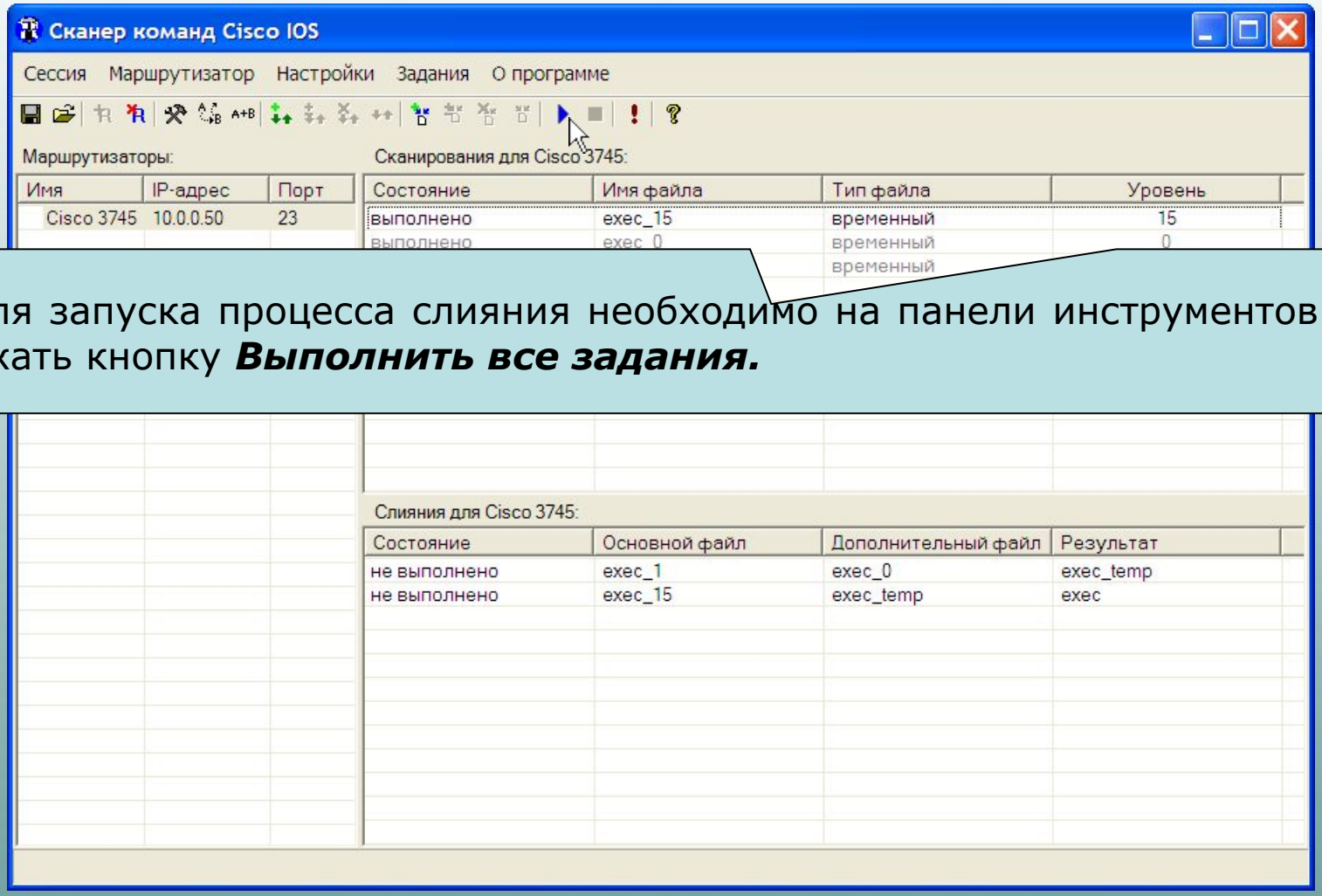
Задание параметров слияния



Для получения результирующего файла, который будет содержать набор команд маршрутизатора для базы данных «ЭФРОС», необходимо объединить команды 15 и 0&1 уровней.

© ООО «Газинформсервис»

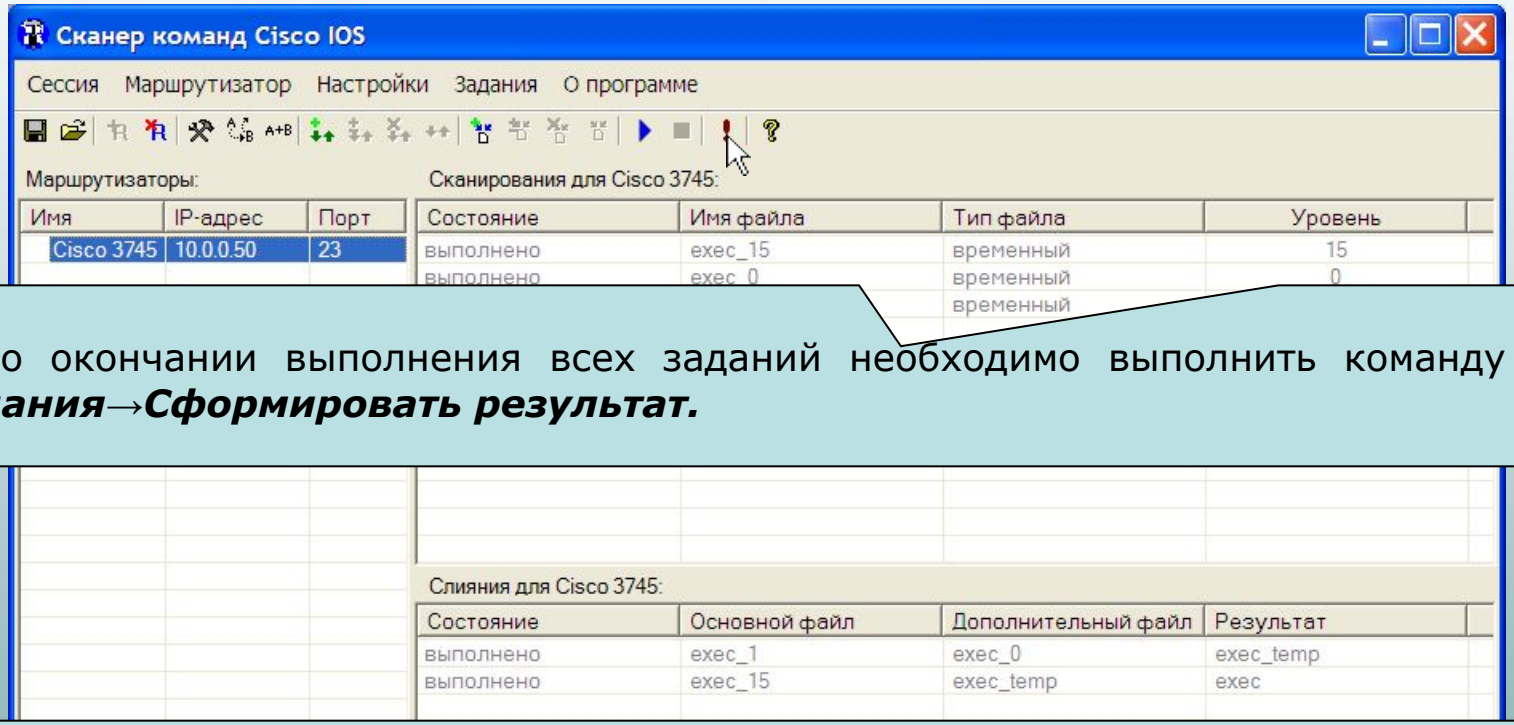
Начало процесса слияния



Для запуска процесса слияния необходимо на панели инструментов нажать кнопку ***Выполнить все задания.***

© ООО «Газинформсервис»

Формирование окончательного результата



По окончании выполнения всех заданий необходимо выполнить команду ***Задания→Сформировать результат.***

По этой команде формируется результирующий файл, содержащий команды маршрутизатора для базы данных ИК «ЭФРОС». Результаты слияния помещаются в каталоги
../<место установки>/Эфрос-сканер/Routers/Cisco 3745/Modes
../<место установки>/Эфрос-сканер/Routers/Cisco 3745/Comments.

© ООО «Газинформсервис»

Просмотр результата

exec.txt - Блокнот

Файл Правка Формат Вид Справка

```
1 x28 escape WORD
1 x28 escape WORD debug
1 x28 escape WORD dns
1 x28 escape WORD noescape
1 x28 escape WORD nuicud
1 x28 escape WORD profile WORD
1 x28 escape WORD profile WORD debug
1 x28 escape WORD profile WORD dns
1 x28 escape WORD profile WORD noescape
1 x28 escape WORD profile WORD nuicud
1 x28 escape WORD profile WORD reverse
1 x28 escape WORD profile WORD verbose
1 x28 escape WORD reverse
1 x28 escape WORD verbose
1 x28 noescape
1 x28 nuicud
1 x28 profile WORD
1 x28 profile WORD debug
1 x28 profile WORD dns
1 x28 profile WORD escape
1 x28 profile WORD escape WORD
1 x28 profile WORD escape WORD debug
1 x28 profile WORD escape WORD dns
1 x28 profile WORD escape WORD noescape
```

Результат работы программы можно посмотреть в каталогах:
../<место установки>/Эфрос-сканер/Routers/Cisco 3745/Modes и
../<место установки>/Эфрос-сканер/Routers/Cisco 3745/Comments.
В папке comments находится файл с комментариями.

© ООО «Газинформсервис»