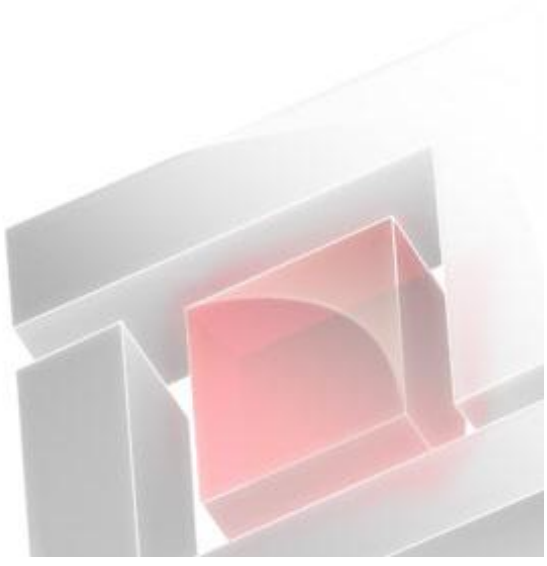
ALTELL
IT Innovations & Security

Altell NEO

Краткое руководство по настройке



Санкт-Петербург 2014

1 Подключение Altell NEO

1.1 Настройки по умолчанию

Для работы с интерфейсом устройства необходимо пройти процедуру аутентификации с использованием идентификатора учётной записи пользователя и пароля. По умолчанию в системе уже есть одна предварительно определённая учётная запись пользователя со следующими параметрами:

идентификатор: **admin**
пароль: **admin**

Пароль для данной учётной записи необходимо изменить сразу же после начала использования системы.

По умолчанию удалённый доступ к Altell NEO разрешён только через управляющий порт Altell NEO. Расположение управляющего порта зависит от модели устройства. На корпусе устройства управляющий порт обозначен номером **1** или как **ethm.** Схема расположения портов для разных моделей NEO приведена в разделе 8, стр. 22.

1.2 Получение доступа для управления

Для управления Altell NEO можно использовать как интерфейс командной строки, так и графический пользовательский веб-интерфейс.

По умолчанию веб-интерфейс доступен только на управляющем порту. Интерфейс командной строки доступен и на управляющем порту, и при подключении через последовательный порт.

1.2.1 Доступ через последовательный порт

При подключении через последовательный порт (RS232) используются следующие параметры:

— скорость 115200 бит/с;
— без контроля чётности (No parity);
— 8 бит данных (8 data bits);
— 1 стоповый бит (1 stop bit).

Для подключения можно использовать любой терминальный клиент работающий с последовательным портом, для Windows можно воспользоваться клиентом поставляемым на компакт-диске (см. раздел 5, стр. 20), для UNIX-подобных систем можно воспользоваться такими программами как minicom, picocom или screen.

При подключении через последовательный порт могут возникнуть проблемы при отображении кириллических символов.

1.2.2 Подключение к управляющему порту

Для получения удалённого доступа следует соединить порт Ethernet управляющего компьютера с управляющим портом Altell NEO при помощи кабеля (UTP категории 5), который входит в комплект поставки. При непосредственном подключении (без использования коммутатора) рекомендуется использовать патч-корд с перекрёстной

разводкой, во избежание возможных проблем в случае отсутствия на управляющем компьютере поддержки автоопределения MDI/MDI-X.

В качестве управляющего компьютера может быть использован любой персональный компьютер или ноутбук, оснащённый 10Base-T/100Base-TX совместимым адаптером Ethernet.

Выбранный для связи с управляющим портом интерфейс Ethernet управляющего компьютера следует настроить на автоматическое получение адреса по DHCP, в результате чего устройством будет выдана конфигурация, достаточная для доступа к интерфейсу управления Altell NEO.

По умолчанию управляющий порт NEO настроен на сеть 192.168.200.0/24 и имеет собственный адрес **192.168.200.1.** Этот адрес должен использоваться для доступа к интерфейсам управления.

1.2.2.1 Доступ к интерфейсу командной строки по протоколу SSH

Для обеспечения безопасной передачи данных по протоколу SSH используется шифрование на основе стандарта ГОСТ 28147—89, а также аутентификация на основе стандарта ГОСТ 34.10—2001. По этой причине на управляющем компьютере должен использоваться клиент SSH, поддерживающий указанные криптографические алгоритмы. Клиентов SSH для разных операционных систем можно найти на компакт-диске (см. раздел 5, стр. 20).

1.2.2.2 Доступ к веб-интерфейсу

В случае веб-интерфейса безопасность передачи данных обеспечивается протоколом HTTPS, использующим шифрование на основе стандарта ГОСТ 28147—89, а также аутентификацию на основе стандарта ГОСТ 34.10—2001. По этой причине на управляющем компьютере должен использоваться веб-браузер, поддерживающий указанные криптографические алгоритмы. Веб-браузер с поддержкой ГОСТ для разных операционных систем можно найти на компакт-диске (см. раздел 5, стр. 20).

2 Пользовательский интерфейс

2.1 Интерфейс командной строки

2.1.1 Режимы команд

Интерфейс командной строки Altell NEO может находиться в двух режимах работы — эксплуатационном и настроечном:

- в эксплуатационном режиме обеспечивается доступ к командам отображения и очистки текущего состояния устройства, отображения конфигурации, включения или выключения отладки, настройки параметров терминалов, сохранения и загрузки состояния, а также перезапуска устройства;
- в настроечном режиме обеспечивается доступ к командам создания, изменения и удаления элементов конфигурации, а также к командам переходов по иерархии параметров.

По умолчанию, при входе в систему интерфейс находится в эксплуатационном режиме. Для перехода из эксплуатационного режима в режим настройки используется команда **configure.**

Для возврата из режима настройки в эксплуатационный режим используется команда **exit.** Переход в эксплуатационный режим при незафиксированных изменениях в конфигурации не допускается, о чём устройство выдаёт соответствующее предупреждение. В этом случае, изменения необходимо либо применить с помощью команды **commit,** либо отменить с помощью команды **discard** (или выходить из режима настройки с помощью команды **exit discard**).

При выполнении команды **exit** в эксплуатационном режиме происходит выход из системы.

Когда устройство ожидает ввода команд, оно показывает соответствующее приглашение, которое также информирует пользователя о том, в каком режиме он работает с командной строкой, от имени какой учетной записи он работает и каково имя системы:

`admin@neo:~$`	Учётная запись: **admin** Имя системы: **neo** Режим интерфейса: эксплуатационный (значок «$»)
`[edit policy]` `admin@gate4#`	Учётная запись: **admin** Имя системы: **gate4** Режим интерфейса: настроечный (значок «#») Ветвь конфигурации: policy

2.1.2 Автодополнение команд

В интерфейсе командной строки имеется функция автодополнения вводимых команд по первым введённым символам. Она задействуется клавиатурными комбинациями, описанными в таблице 1:

Таблица 1: Клавиши автодополнения

Нажатые клавиши	**Результат**
<Tab>	Автодополнение команды: — если введённые символы можно дополнить однозначно, до единственной команды, то это и происходит; — если возможен более чем один вариант автодополнения, то система отображает список возможных последующих команд. При повторном нажатии клавиши <Tab> отображается справка интерфейса командной строки для списка возможных последующих команд.
?	При нажатии на клавишу с вопросительным знаком («?») также выполняется автодополнение команды. Для «обычного» ввода символа вопросительного знака, следует сначала нажать <Ctrl>+v, потом вопросительный знак.

2.2 Веб-интерфейс

Веб-интерфейс является альтернативным интерфейсом пользователя для взаимодействия с Altell NEO.

Все операции, которые пользователь может выполнить с помощью интерфейса командной строки, доступны и в веб-интерфейсе. Веб-интерфейс, фактически, отражает структуру интерфейса командной строки. В частности, иерархия команд, представленных в веб-интерфейсе, совпадает с иерархией конфигурации в интерфейсе командной строки.

2.2.1 Структура веб-интерфейса

Графический интерфейс пользователя разделён на 4 области: заголовок, область навигации, командные кнопки, область ввода/вывода (рис. 1).

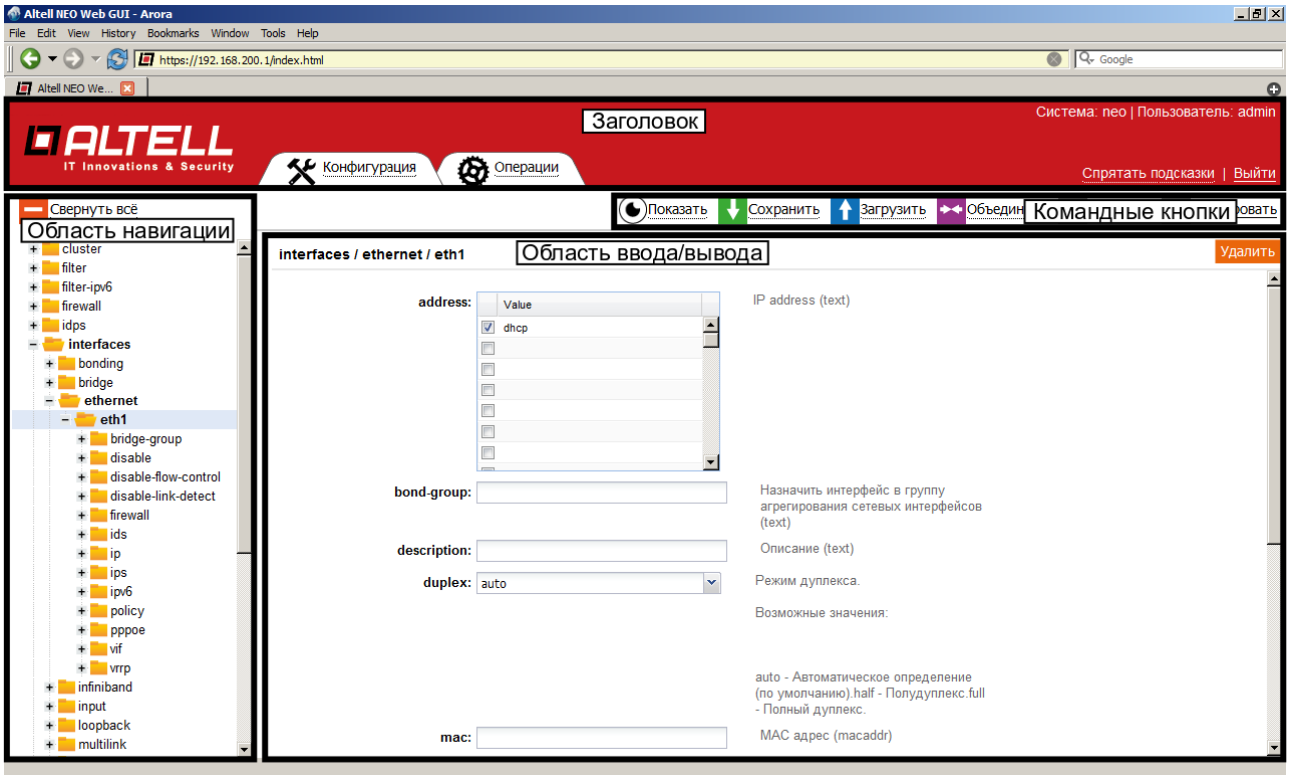


Рис. 1: Структура веб-интерфейса

2.2.1.1 Заголовок

Область заголовка расположена в верхней части окна веб-интерфейса. В этой области отображается логотип, имя узла, идентификатор учётной записи, от имени которой выполнен вход в систему, кнопки **Выход** и **Спрятать подсказки/Показать подсказки,** а также две основные вкладки: **Конфигурация** и **Операции.**

2.2.1.2 Область навигации

В левой части окна веб-интерфейса расположена область навигации, которая представляет собой иерархическое меню, отображающее структуру команд интерфейса

командной строки. Если выбрана вкладка **Конфигурация,** то отображается иерархическое дерево команд настройки, если выбрана вкладка **Операции,** то отображается иерархическое дерево эксплуатационных команд.

2.2.1.3 Командные кнопки

Область командных кнопок расположена между заголовком и областью ввода/вывода. Перечень доступных командных кнопок определяется выбранным режимом.

Выбор вкладки **Конфигурация** открывает следующие командные кнопки:

- **Показать** — показ текущей конфигурации системы;
- **Сохранить** — сохранение текущей конфигурации в файл;
- **Загрузить** — загрузка ранее сохранённой конфигурации;
- **Объединить** — слияние ранее сохранённой конфигурации с текущей конфигурацией;
- **Сбросить** — отмена всех незафиксированных изменений в конфигурации;
- **Фиксировать** — фиксация всех имеющихся изменений в конфигурации.

При выборе вкладки **Операции,** командные кнопки отсутствуют.

2.2.1.4 Область ввода/вывода

Область ввода/вывода расположена справа от области навигации. В этой области отображаются поля ввода и вывода системной информации.

Фон полей параметров, значение которых было изменено, но не зафиксировано, подсвечивается. Изменение параметра в веб-интерфейсе аналогично применению команды **set** в интерфейсе командной строки. Изменение параметра в веб-интерфейсе происходит в следующих случаях:

- при нажатии на клавишу <Enter>;
- при нажатии на кнопку **Установить.**

2.2.2 Навигация по дереву конфигурации

Веб-интерфейс предоставляет вспомогательные средства, облегчающие навигацию при настройке:

- *перемещение по дереву конфигурации.* Перемещаться по иерархическому дереву конфигурации можно следующими способами:
  - щёлкнуть имя узла. При щелчке имени требуемого узла, в области навигации отобразится следующий уровень дерева конфигурации, при этом в области ввода/вывода будут отображены поля с параметрами, соответствующими выбранному уровню иерархии;
  - щёлкнуть значок «+/−». При щелчке значка «+» в области навигации отобразится следующий уровень дерева конфигурации для выбранного узла, но при этом никакой дополнительной информации в области ввода/вывода отображено не будет. При щелчке значка «−» все уровни дерева конфигурации будут свернуты до выбранного.

— *жёлтые маркеры.* Жёлтые маркеры отображаются в областях навигации и ввода/вывода, отмечая незафиксированные изменения в конфигурации. Жёлтые маркеры отображаются для всех уровней изменённой ветви дерева конфигурации и помечают параметры по следующим правилам:
  — изменение значения существующего параметра отмечается простым жёлтым маркером;
  — новый параметр конфигурации отмечается жёлтым маркером со знаком «+».
  — удалённый из конфигурации параметр отмечается жёлтым маркером со знаком «–».

  Жёлтые маркеры будут сняты при нажатии на кнопку **Сбросить** (с отменой внесённых изменений) или кнопку **Фиксировать** (с фиксацией внесённых изменений).

  Примечание. Все незафиксированные изменения конфигурации сохраняются в течении сессии пользователя и видны всем пользователям, вошедшим в систему.
— *красные маркеры.* Красные маркеры отображаются в областях навигации и ввода/вывода и помечают обязательные параметры, значение для которых не было установлено;
— *названия узлов конфигурации, выделенные полужирным шрифтом.* В иерархическом дереве конфигурации полужирным шрифтом выделяются названия узлов, изменение которых было зафиксировано.

2.2.3 Использование документации к интерфейсу командной строки

Основная часть документации Altell NEO описывает работу с интерфейсом командной строки. При этом, примеры, приведённые для интерфейса командной строки, можно выполнять и в веб-интерфейсе, так как оба интерфейса предоставляют одну и ту же функциональность.

Все команды режима настройки доступны при выборе вкладки **Конфигурация,** команды эксплуатационного режима — при выборе вкладки **Операции.** При щелчке названия узла в области навигации отображается следующий уровень команд в иерархии конфигурации, а в области ввода/вывода отображаются поля для ввода значений соответствующих параметров.

Например, в интерфейсе командной строки выполняются следующие команды:

```
[edit]
admin@neo# set interfaces ethernet eth1 address 192.168.1.61/24
[edit]
admin@neo# commit
```

Для выполнения этих команд в веб-интерфейсе (рис. 2), необходимо выполнить следующие действия:

1. Выбрать вкладку **Конфигурация.**
2. Выбрать в области навигации узлы **interfaces>ethernet>eth1,** щёлкнуть название узла **eth1.**
3. Ввести адрес 192.168.1.61/24 в поле **address** области ввода/вывода и установить флаг в поле рядом с указанным адресом.
4. Нажать на клавишу <Enter> или на кнопку **Установить,** после чего появится жёлтый маркер.

5. Нажать на кнопку **Фиксировать** для применения внесённых изменений, после чего жёлтые маркеры будут сняты.

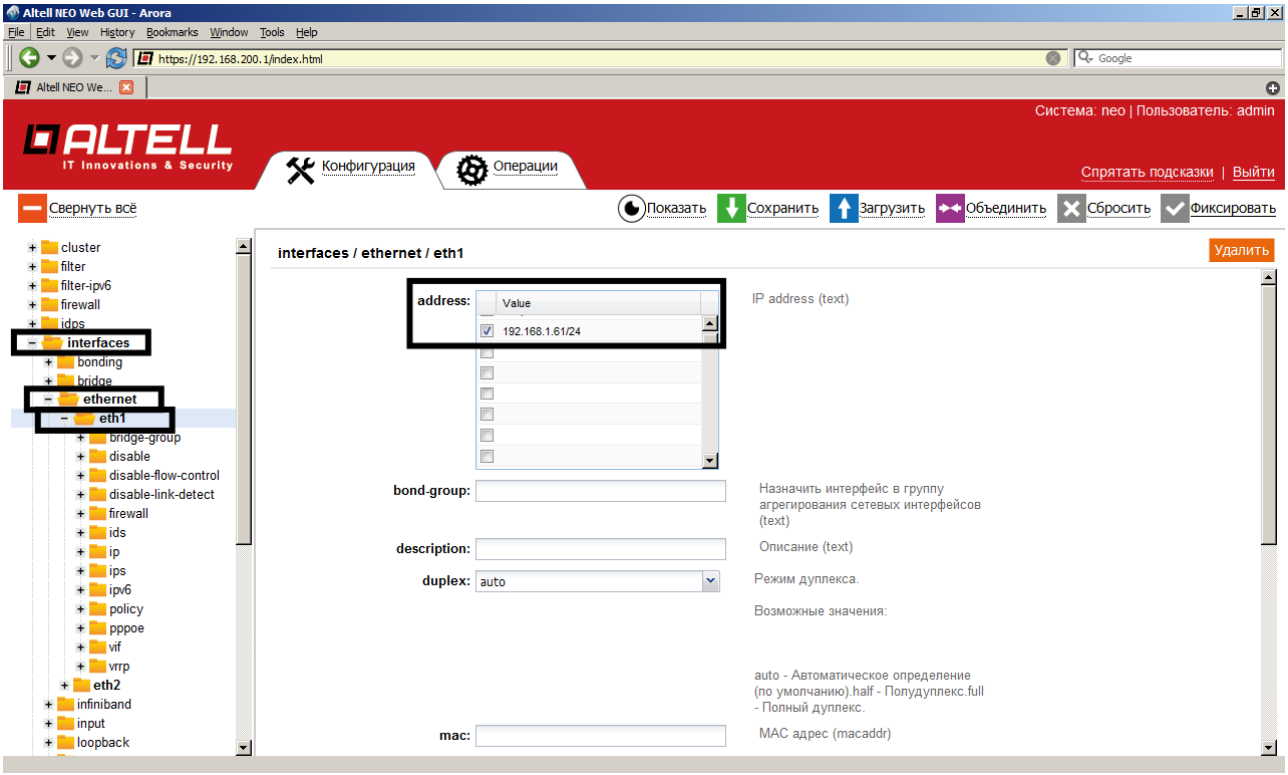


Рис. 2: Настройка сетевых интерфейсов через веб-интерфейс

3 Конфигурация

3.1 Общие сведения по конфигурации

3.1.1 Иерархия дерева конфигурации

Конфигурация устройства имеет древовидное строение и разделяется логически на узлы и атрибуты конфигурации. *Атрибут* конфигурации имеет вид *атрибут значение,* как в приведённом ниже примере:

```
protocol-version v2
```

У *узла* конфигурации всегда есть закрытая пара фигурных скобок, содержимое которой может быть пусто, как в следующем примере:

```
dns-server ipv4 {
}
```

или непусто, как в следующем примере:

```
ssh {
    allow-root
}
```

3.1.2 Добавление параметров к конфигурации или изменение конфигурации

Добавление нового параметра производится в режиме настройки через создание атрибутов и узлов конфигурации командой **set.** Изменение существующего параметра выполняется тоже в режиме настройки с помощью команды **set,** как в приведённом ниже примере:

```
[edit]
admin@neo# set interfaces ethernet eth2 address 192.168.1.100/24
```

Затем для просмотра изменений можно использовать команду **show:**

```
[edit]
admin@neo# show interfaces ethernet eth2
+address 192.168.1.100/24
```

Обратите внимание на знак «+» перед новым оператором. Он показывает, что оператор был добавлен к конфигурации, но изменение ещё не зафиксировано. Изменение не вступит в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды **commit.**

Конфигурацию можно изменять начиная с корня дерева конфигурации или использовать команду **edit** для перемещения к той ветви дерева, в которой надо выполнить изменения, а также команды **up** и **top** для возврата на верхние уровни.

При первой загрузке системы дерево конфигурации практически пусто, за исключением нескольких автоматически настроенных узлов. Вся функциональность системы настраивается через создание и изменение узлов и атрибутов конфигурации. Когда создаётся новый узел, для всех его атрибутов применяются значения по умолчанию.

3.1.3 Удаление параметров

Для удаления атрибута или целого узла в настройке служит команда **delete,** как в приведённом ниже примере:

```
[edit]
admin@neo# delete interfaces ethernet eth2 address 192.168.1.100/24
```

Затем для просмотра изменений можно использовать команду **show:**

```
[edit]
admin@neo# show interfaces ethernet eth2
-address 192.168.1.100/24
```

Обратите внимание на знак «–» перед удалённым атрибутом. Он показывает, что атрибут был удалён из конфигурации, но изменение еще не зафиксировано. Изменение не вступит в силу до тех пор, пока конфигурация не будет зафиксирована с помощью команды **commit.**

Некоторые узлы и атрибуты конфигурации являются обязательными, среди них есть такие, которые нельзя удалить, а есть имеющие значения по умолчанию, при удалении которых для них будет восстановлено это значение.

3.1.4 Фиксация изменений конфигурации

Изменения в конфигурации вступают в силу только после их фиксации командой **commit:**

```
[edit]
admin@neo# commit
```

При просмотре конфигурации имеющиеся незафиксированные изменения помечаются знаком «+» (в случае добавления/правки) или «–» (в случае удаления). При фиксации изменений знаки удаляются, как в приведённом ниже примере:

```
[edit]
admin@neo# show interfaces ethernet eth2
-address 192.168.1.100/24
[edit]
admin@neo# commit
[edit]
admin@neo# show interfaces ethernet eth2
```

Изменения фиксируются в текущей (активной) конфигурации. Для того чтобы полученная конфигурация использовалась после перезагрузки устройства она должна быть сохранена в файл командой save, *см. раздел 3.1.6, стр. 10.*

3.1.5 Отмена изменений в конфигурации

Выйти из режима настройки при наличии незафиксированных изменений невозможно: необходимо либо фиксировать изменения, либо отказаться от них. Если фиксировать изменения не нужно, можно отменить их с помощью команды **exit discard:**

```
[edit]
admin@neo# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
[edit]
admin@neo# exit discard
```

3.1.6 Сохранение конфигурации в файл

Действующую в данный момент конфигурацию можно сохранить в файл при помощи команды **save** в режиме настройки. По умолчанию, конфигурация сохраняется в файл **config.boot** в стандартном каталоге конфигурации, которым является **/etc/config:**

```
[edit]
admin@neo# save
Запись конфигурации в '/etc/config/config.boot'...
Готово
```

При включении питания устройство загружает конфигурацию именно из файла **/etc/config/config.boot,** поэтому после успешной настройки всех необходимых сервисов важно сохранить текущую конфигурацию в этот файл.

Можно сохранить конфигурацию под другим именем, указав другое имя файла:

```
[edit]
admin@neo# save testconfig
Запись конфигурации в '/etc/config/testconfig'...
Готово
```

Кроме того, для сохранения файла конфигурации можно указать и другой каталог, отличный от стандартного **/etc/config.** Сохранять можно на жесткий диск, карту CF или USB-накопитель, включив точку монтирования носителя в путь. Также поддерживается сохранение файла на сервера FTP, TFTP или HTTP.

В таблице 2 приведены поддерживаемые устройством пути для сохранения файла конфигурации:

Таблица 2: Способы указания местоположения файла конфигурации

Местоположение	**Способ указания**
Абсолютный путь	Используется стандартный способ указания файла в UNIX.
Относительный путь	Указывается имя файла относительно стандартного каталога */etc/config*.
Сервер TFTP	Используется следующий синтаксис для имени файла: *tftp://ip-адрес/файл_конфигурации*, где *ip-адрес* это IP-адрес сервера TFTP, а *файл_конфигурации* это файл конфигурации, включая путь относительно корневого каталога TFTP.
Сервер FTP	Используется следующий синтаксис для имени файла: *ftp://ip-адрес/файл_конфигурации*, где *ip-адрес* это IP-адрес сервера FTP, а *файл_конфигурации* это файл конфигурации, включая путь. При использовании FTP будет выдан запрос на ввод имени учётной записи на сервере FTP и её пароля.
Сервер HTTP	Используется следующий синтаксис для имени файла: *http://ip-адрес/файл_конфигурации*, где *ip-адрес* это IP-адрес сервера HTTP, а *файл_конфигурации* это файл конфигурации, включая путь.

Перед тем, как конфигурацию можно будет сохранить на флэш-накопитель, последний следует смонтировать командой **flash mount** в эксплуатационном режиме.

Обратите внимание, что команда **save** записывает только актуальную конфигурацию. При наличии незафиксированных изменений система выдаст предупреждение о том, что она сохраняет только фиксированные изменения.

3.1.7 Загрузка конфигурации

Для загрузки ранее сохранённой конфигурации используется команда **load** в режиме настройки. По умолчанию система считывает файл из стандартного каталога конфигурации — **/etc/config:**

```
[edit]
admin@neo# load testconfig
Loading config file /etc/config/testconfig... Done
```

Загруженная конфигурация автоматически применяется и становится активной конфигурацией.

3.2 Пример. Базовая конфигурация

В этом разделе приведён пример начальной настройки системы. Для доступа к интерфейсу командной строки используется протокол SSH. Работа ведётся от имени учетной записи, определённой по умолчанию: идентификатор пользователя — **admin,** пароль — **admin.**

3.2.1 Переход в режим настройки

После входа в систему мы оказываемся в эксплуатационном режиме, являющимся режимом по умолчанию:

```
Last login: Wed Dec 29 11:12:58 2010 from 192.168.200.2
admin@neo:~$
```

Для настройки системы необходимо перейти в режим настройки:

```
admin@neo:~$ configure
[edit]
admin@neo#
```

3.2.2 Установка имени системы

По умолчанию системе присвоено имя **neo.** При необходимости это значение можно изменить:

```
[edit]
admin@neo# set system host-name border
[edit]
admin@neo# commit
```

Вид приглашения, соответствующий новому имени системы, появится при следующем входе в систему.

3.2.3 Установка имени домена

В дополнение к изменению имени системы, может потребоваться изменить имя домена:

```
[edit]
admin@neo# set system domain-name test.ru
[edit]
admin@neo# commit
```

3.2.4 Изменение пароля

По умолчанию в системе есть одна предварительно определённая учётная запись пользователя:

— идентификатор пользователя: **admin;**

— пароль по умолчанию: **admin.**

Пароль для данной учётной записи необходимо изменить сразу же после начала использования системы:

```
[edit]
admin@neo# set system login user admin authentication \
plaintext-password '98V$jngpsvn45'
[edit]
admin@neo# commit
```

3.2.5 Настройка интерфейсов

Тип и номер изменяемого интерфейса зависят от используемого устройства и топологии сети. Однако, практически при любой топологии сети требуется настройка по крайней мере одного интерфейса Ethernet. В этом примере приведена настройка интерфейса **eth1** в качестве интерфейса, к которому подключён внешний сегмент сети:

```
[edit]
admin@neo# set interfaces ethernet eth1 address 203.0.113.10/24
[edit]
admin@neo# commit
```

В том случае, когда провайдер предоставляет сетевые настройки по протоколу DHCP, следует использовать команду set interfaces ethernet eth1 address dhcp.

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show interfaces
ethernet eth1 {
    address 203.0.113.10/24
}
management true
```

3.2.6 Настройка маршрута по умолчанию

Получателем трафика, для которого Altell NEO не может определить маршрут исходя из собственных таблиц маршрутизации, является другое внешнее устройство, называемое маршрутизатором по умолчанию (а путь отправки такого трафика называется маршрутом по умолчанию). Адрес маршрутизатора по умолчанию указывается следующим образом:

```
[edit]
admin@neo# set system gateway-address 203.0.113.100
[edit]
admin@neo# commit
```

3.3 Пример. Интернет-шлюз

Рассматриваемая в этом примере конфигурация предполагает следующее:

- настройка маршрутизации сетевого трафика между локальной сетью (LAN) и интернетом;
- возможность получения доступа к Altell NEO по протоколу SSH из внутренней сети;
- назначение адресов устройствам во внутренней локальной сети динамически, по протоколу DHCP;
- использование ретрансляции DNS для устройств во внутренней локальной сети;
- использование NAT для преобразования внутренних адресов в один внешний адрес;

— настройка межсетевого экрана для предотвращения доступа к системе из внешнего сегмента сети (интернета).

В данном примере приведена настройка двух интерфейсов Ethernet, к одному из которых **(eth1)** подключён внешний сегмент сети (WAN), а к другому **(eth2)** подключён локальный сегмент сети (LAN), как показано на рис. 3.

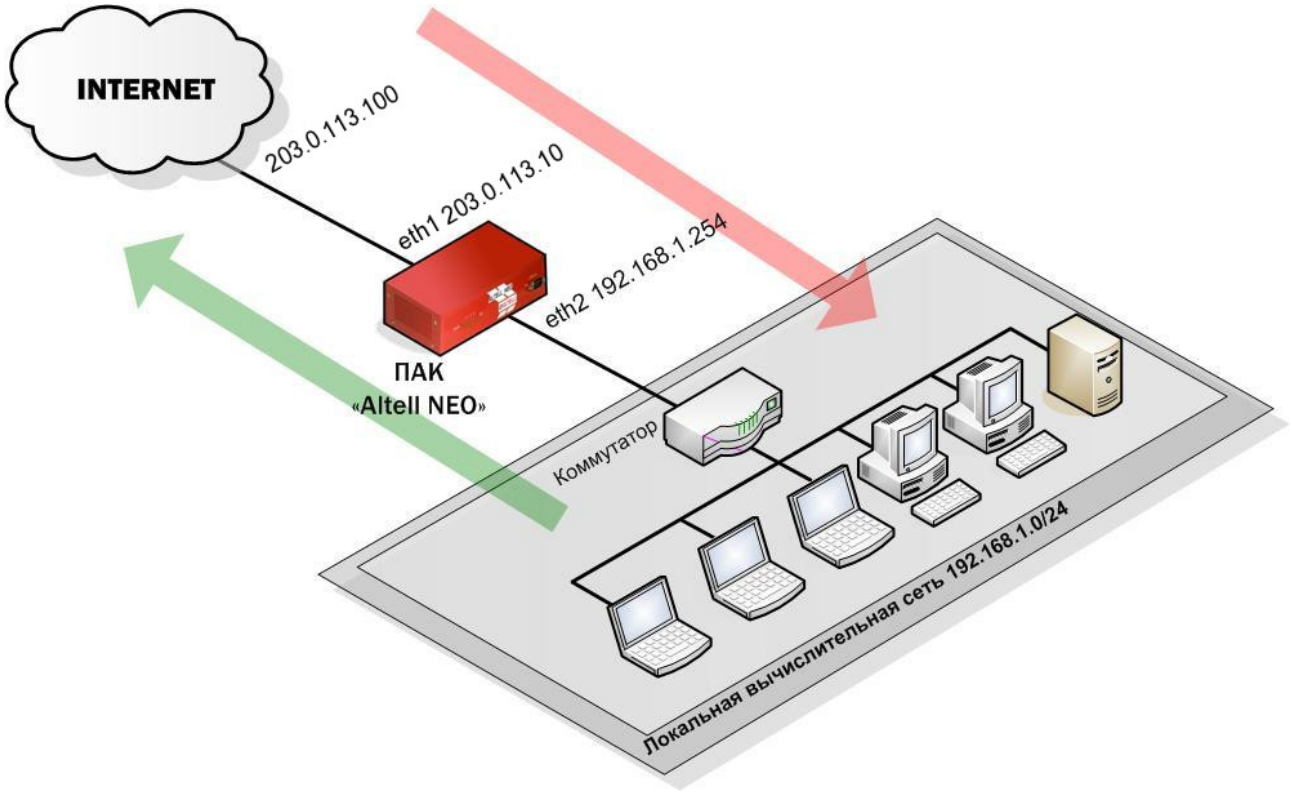


Рис. 3: Интернет-шлюз

В этом примере также предполагается, что уже выполнена настройка из предыдущего примера.

3.3.1 Настройка интерфейсов

В предыдущем примере был настроен внешний интерфейс **eth1.** Для того, чтобы Altell NEO функционировал в качестве интернет-шлюза, в системе необходимо настроить ещё один интерфейс, к которому будет подключён локальный сегмент сети (LAN). В нашем случае используется интерфейс **eth2:**

```
[edit]
admin@neo# set interfaces ethernet eth2 address 192.168.1.254/24
[edit]
admin@neo# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show interfaces
ethernet eth1 {
    address 203.0.113.10/24
}
```

```
ethernet eth2 {
    address 192.168.1.254/24
}
management true
```

3.3.2 Включение доступа по протоколу SSH

По умолчанию доступ к Altell NEO по протоколу SSH разрешён только на управляющем интерфейсе. Доступ из локальной сети включается следующей командой:

```
[edit]
admin@neo# set service ssh address 192.168.1.254
[edit]
admin@neo# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show service ssh
   address 192.168.1.254 {
   }
   cipher gost89
   hmac hmac-gosthash
   hmac hmac-gosthash2012-256
   key-exchange-algo diffie-hellman-ec-gost94
```

3.3.3 Настройка сервера DHCP

Протокол динамической настройки системы (Dynamic Host Configuration Protocol, DHCP) обеспечивает динамическое назначение IP-адресов и других сведений о настройке системам указанного сегмента сети. В нашем примере сервер DHCP обеспечивает динамическое назначение IP-адресов компьютерам в локальной сети (LAN).

В настройке сервера DHCP необходимо определить перечень (блок/пул) адресов, которые будут выдаваться клиентам в локальной сети (192.168.1.100—192.168.1.199). В качестве маршрутизатора по умолчанию будет указываться адрес внутреннего интерфейса **(eth2)** Altell NEO:

```
[edit]
admin@neo# set service dhcp-server subnet 192.168.1.0/24 \
start 192.168.1.100 stop 192.168.1.199
[edit]
admin@neo# set service dhcp-server subnet 192.168.1.0/24 \
default-router 192.168.1.254
[edit]
admin@neo# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show service dhcp-server
subnet 192.168.1.0/24 {
    start 192.168.1.100 {
        stop 192.168.1.199
```

```
    }
    default-router 192.168.1.254
}
```

3.3.4 Настройка DNS

3.3.4.1 Системный сервер DNS

Настраиваемый системный сервер DNS будет использоваться самим Altell NEO и всеми его сервисами для разрешения имён. Обычно указывается предоставленный провайдером сервер DNS. В отсутствие настройки конкретного используемого сервера DNS будут использоваться сервера, получаемые с помощью протокола DHCP, либо полученные через туннели PPPoE, PPTP, OpenVPN и т.п. Статическая настройка использования конкретного сервера выполняется следующим образом:

```
[edit]
admin@neo# set system name-server 203.0.113.100
[edit]
admin@neo# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show system name-server
 name-server 203.0.113.100
```

3.3.4.2 Сервис ретрансляции DNS

Сервис ретрансляции DNS позволяет клиентам локальной сети использовать Altell NEO для разрешения имён посредством протокола DNS. По умолчанию, сам сервис использует доступные системные сервера DNS, а настройка доступа требует указания интерфейса. В данном примере необходимо указать внутренний интерфейс **(eth2):**

```
[edit]
admin@neo# set service dns forwarding listen-on eth2
[edit]
admin@neo# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show service dns forwarding
   listen-on eth2
```

3.3.5 Настройка NAT

Интернет-шлюз должен отправлять исходящий сетевой трафик из локальной сети через внешний интерфейс и заменять внутренние адреса на внешний общедоступный адрес. Для этого необходимо определить правило NAT.

Определим правило, обеспечивающее прохождение трафика из внутренней подсети 192.168.1.0/24 в интернет через интерфейс **eth1** и заменяющее внутренние адреса на внешний адрес интерфейса **eth1:**

```
[edit]
admin@neo# set service nat rule 1 source address 192.168.1.0/24
[edit]
admin@neo# set service nat rule 1 outbound-interface eth1
[edit]
admin@neo# set service nat rule 1 type masquerade
[edit]
admin@neo# commit
```

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show service nat
rule 1 {
    type masquerade
    outbound-interface eth1
    source {
        address 192.168.1.0/24
    }
}
```

3.3.6 Настройка межсетевого экрана (МЭ)

При настройках по умолчанию Altell NEO никак не ограничивает прохождение сетевого трафика. Передача трафика через интерфейс разрешена до тех пор, пока к интерфейсу не будет применено правило МЭ. В данном примере интернет-шлюз должен разрешать доступ к интернету устройствам из локальной сети и собственным службам, но необходимо блокировать трафик, инициированный источниками из внешнего сегмента сети.

В общем случае, для настройки правил МЭ на интерфейсе необходимо сделать следующее:

- определить поименованные наборы правил МЭ (т.н. экземпляры МЭ), каждый из которых может содержать одно или более правил;
- применить необходимые экземпляры МЭ к интерфейсу. Экземпляр МЭ может фильтровать пакеты одного из следующих направлений:
  - **in** (входящий). Если применить экземпляр с использованием ключевого слова **in,** то межсетевой экран будет фильтровать пакеты, входящие в интерфейс и транзитно проходящие через устройство;
  - **out** (исходящий). Если применить экземпляр с использованием ключевого слова **out,** то межсетевой экран будет фильтровать транзитные пакеты проходящие через устройство, и покидающие её через указанный интерфейс;
  - **local** (локальный). Если применить экземпляр с использованием ключевого слова **local,** то межсетевой фильтр будет фильтровать пакеты, предназначенные самому устройству (не транзитные).

  При этом, для одного направления трафика может быть применён только один экземпляр МЭ.

3.3.6.1 Определение экземпляра МЭ

Создание правила для пропуска в локальный сегмент сети только ответного трафика, порождённого исходящим трафиком этого сегмента (т.е. установленными *из LAN наружу* соединениями и связанным с ними трафиком):

```
[edit]
admin@neo# set firewall name ALLOW_ESTABLISHED
[edit]
admin@neo# set firewall name ALLOW_ESTABLISHED rule 10
[edit]
admin@neo# set firewall name ALLOW_ESTABLISHED rule 10 action \
    accept
[edit]
admin@neo# set firewall name ALLOW_ESTABLISHED rule 10 state \
    established enable
[edit]
admin@neo# set firewall name ALLOW_ESTABLISHED rule 10 state \
    related enable
[edit]
admin@neo# commit
```

3.3.6.2 Применение экземпляра МЭ к интерфейсу

Применение набора правил ALLOW_ESTABLISHED к сетевому трафику, приходящему на интерфейс:

```
[edit]
admin@neo# set interfaces ethernet eth1 firewall in name \
    ALLOW_ESTABLISHED
[edit]
admin@neo# set interfaces ethernet eth1 firewall local name \
    ALLOW_ESTABLISHED
[edit]
admin@neo# commit
```

> *Если в разделе 3.2.5 использовалась настройка внешнего интерфейса по DHCP, применение МЭ к направлению* local *сделает невозможной конфигурацию интерфейса по DHCP, следует либо не применять соответствующую настройку, либо добавить разрешительные правила для протокола DHCP в МЭ.*

Для просмотра текущей настройки используется команда **show:**

```
[edit]
admin@neo# show firewall
name ALLOW_ESTABLISHED {
    rule 10 {
        action accept
        state {
            established enable
            related enable
        }
```

```
    }
}
```

Просмотр параметров интерфейса:

```
admin@neo# show interfaces ethernet
ethernet eth1 {
    address 203.0.113.21/24
    firewall {
        in {
            name ALLOW_ESTABLISHED
        }
        local {
            name ALLOW_ESTABLISHED
        }
    }
}
ethernet eth2 {
    address 192.168.1.254/24
}
```

4 Обновление программного обеспечения Altell NEO

4.1 Загрузка обновлений

По умолчанию Altell NEO настроен на автоматическую загрузку обновлений программного обеспечения (ПО). Для успешной автоматической загрузки обновлений необходимы следующие условия:

- подключение к интернету;
- корректная настройка системного DNS;
- прохождение входящего трафика с порта 790 протокола TCP (либо входящего трафика для соединений, инициированных самим устройством);

Канал передачи обновлений защищён с помощью протокола TLS со взаимной аутентификацией сторон и шифрованием передаваемых данных. При успешном получении обновления в системный журнал будет добавлена запись от программы *apda* объекта *local1*:

```
admin@neo:~$ show log program apda
Дата       Время    Программа Объект Уров.  Е Сообщение
2014-11-13 14:53:51 apda      local1 warnin 0 Доступно обновление для
программного обеспечения, для его установки необходима перезагрузка
```

4.2 Ручная загрузка обновлений

При отсутствии подключения к интернету обновления можно получить через техническую поддержку (раздел 7, стр. 21) и установить в ручном режиме.

4.3 Установка обновлений

Для установки обновления необходима перезагрузка устройства. При этом, по умолчанию, автоматическое применение обновлений отключено, при поступлении на устройство обновления необходимо выполнить эксплуатационную команду **update on-reboot** и перезагрузить устройство.

Возможна также настройка автоматического применения обновлений при перезагрузке, для этого необходимо сделать следующее:

```
[edit]
admin@neo# set system update-on-reboot true
[edit]
admin@neo# commit
```

5 Содержимое компакт-диска

Компакт-диск содержит каталог «Межсетевой экран Altell NEO», внутри которого находятся файлы и каталоги:

— «quickstartguide.pdf», электронная копия настоящего руководства;

— «Руководство пользователя Altell NEO.pdf», полная пользовательская документация Altell NEO;

— «Документация», каталог, содержащий официальную документацию на ПО и аппаратную часть NEO, а также документацию на веб-браузер и клиент SSH;

— «Сертификаты», каталог с сертификатами NEO (ФСТЭК, ССС, ГОСТ Р, СЭЗ);

— «Клиентское ПО» и «Серверное ПО», каталоги с дополнительным ПО для использования совместно с NEO.

Каталоги ПО разделены по операционным системам, представленный набор ПО поддерживает следующие ОС:

— ALT Linux;

— CentOS;

— Debian;

— Fedora;

— MacOS X;

— Mandriva;

— Red Hat Enterprise Linux;

— Ubuntu;

— Windows;

— openSUSE.

Точные версии поддерживаемых ОС указаны в файлах `README` соответствующих каталогов (кодировка UTF-8 для UNIX-подобных систем и cp1251 для Windows).

Поставляемый набор клиентского ПО состоит из клиента SSH и веб-браузера с поддержкой шифрования ГОСТ (для доступа через веб-интерфейс).

Клиент SSH для Windows может также использоваться для подключения через последовательный порт.

Набор серверного ПО включает в себя схемы LDAP для аутентификации клиентов PPTP/L2TP VPN.

6 Руководство пользователя

Полное руководство пользователя Altell NEO содержится на компакт-диске в каталоге «Межсетевой экран Altell NEO». Документация разбита на несколько глав по описываемой функциональности. В начале каждой главы присутствует вводная часть по рассматриваемой теме с примерами типовых конфигураций.

7 Техническая поддержка

Для создания заявок и переписки с технической поддержкой существует портал, доступный по адресу `https://support.altell.ru/`. Взаимодействовать с технической поддержкой можно также через почту, заявки автоматически создаются для писем, направленных на адрес `support@altell.ru`.

Для ускорения обработки заявок, рекомендуется сопровождать их выводом команды эксплуатационного режима **show tech-support**. Сохранить вывод **show tech-support** на флэш-накопитель вы можете следующим образом:

1. Подключите флэш-накопитель к устройству (накопитель должен быть форматирован в файловую систему FAT или FAT32);

2. Выполните следующие эксплуатационные команды:

```
admin@neo:~$ flash mount
admin@neo:~$ show tech-support save /media/hdd/tech
admin@neo:~$ flash umount
```

3. Извлеките флэш-накопитель из устройства.

В корневом каталоге будет находится файл с именем `tech.[имя_устройства].tech-support.[текущая_дата].gz`, который и необходимо отправить специалистам технической поддержки.

8 Расположение портов на устройствах

Схема расположения портов может отличаться от приведённой, в зависимости от комплектации устройства. В особенности это касается моделей, для которых возможна установка модуля IPMI (310, 340).

Рис. 4: NEO 100

Рис. 5: NEO 110

Рис. 6: NEO 120

Рис. 7: NEO 200

Рис. 8: NEO 210

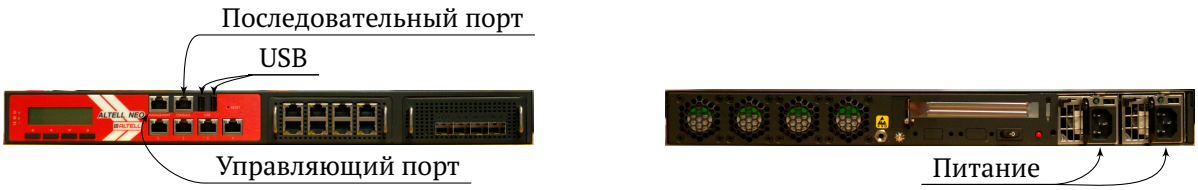


Рис. 9: NEO 310 (без IPMI)

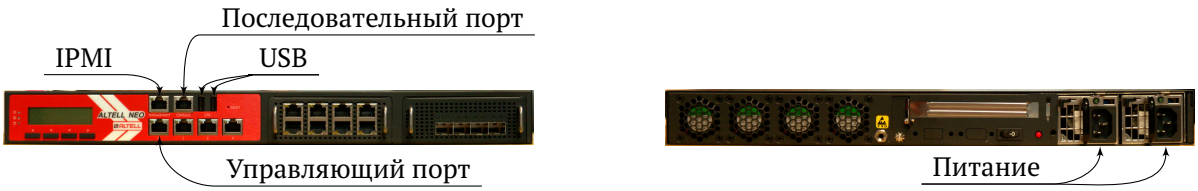


Рис. 10: NEO 310 (с IPMI)

Рис. 11: NEO 340 (без IPMI)

Рис. 12: NEO 340 (с IPMI)