Netgraph/Mpd «изнутри»

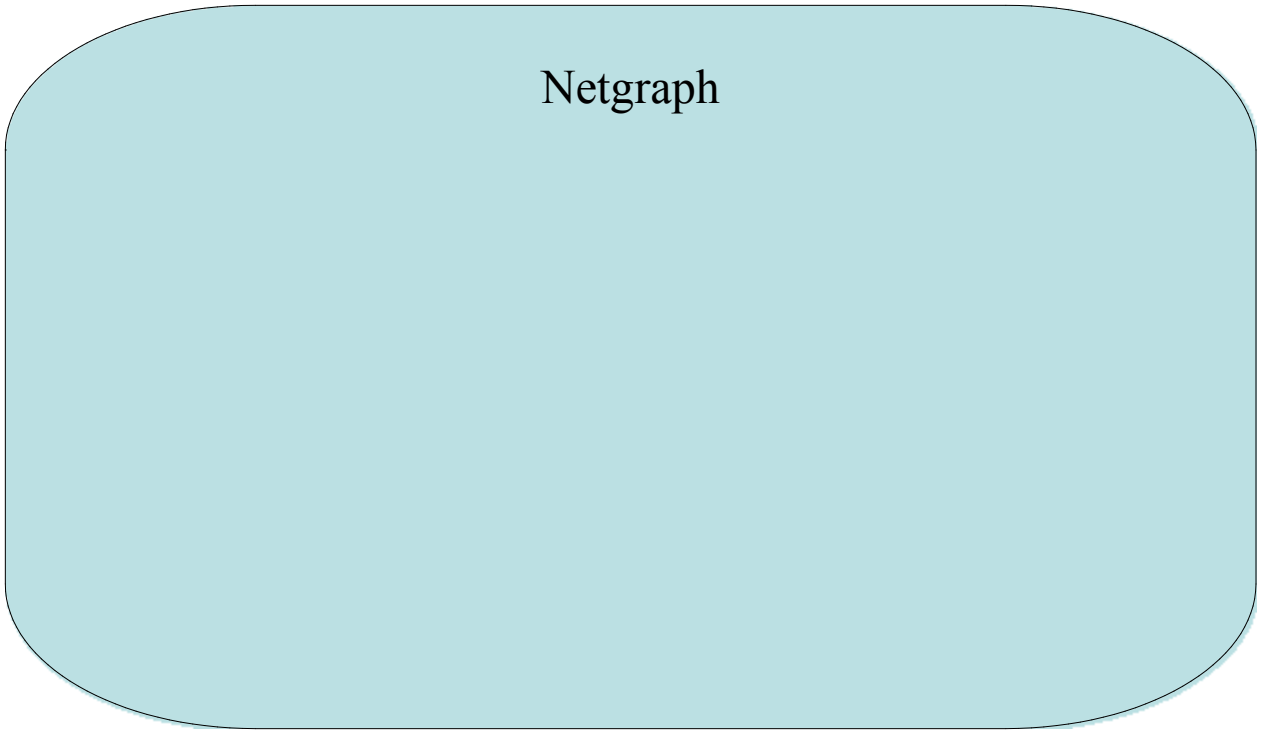
Alexander Motin
mav@FreeBSD.org

- О себе:
  - 1996 - 2002 Днепропетровский Национальный Университет Железнодороджного Транспорта (ДИИТ),
  - 2000 - 2006 ООО «Алькар-Телепорт», ISP, системный администратор, программист отдела биллинга,
  - 2006 - 2007 ООО «Оптима-Телеком», системный администратор, программист отдела интернет биллинга,
  - 2007 - 2009 ОАО «Фарлеп-Инфест», ведущий программист отдела развития клиентского биллинга,
  - с 2003 участвую в проекте Mpd,
  - с 2007 являюсь FreeBSD source коммиттером.

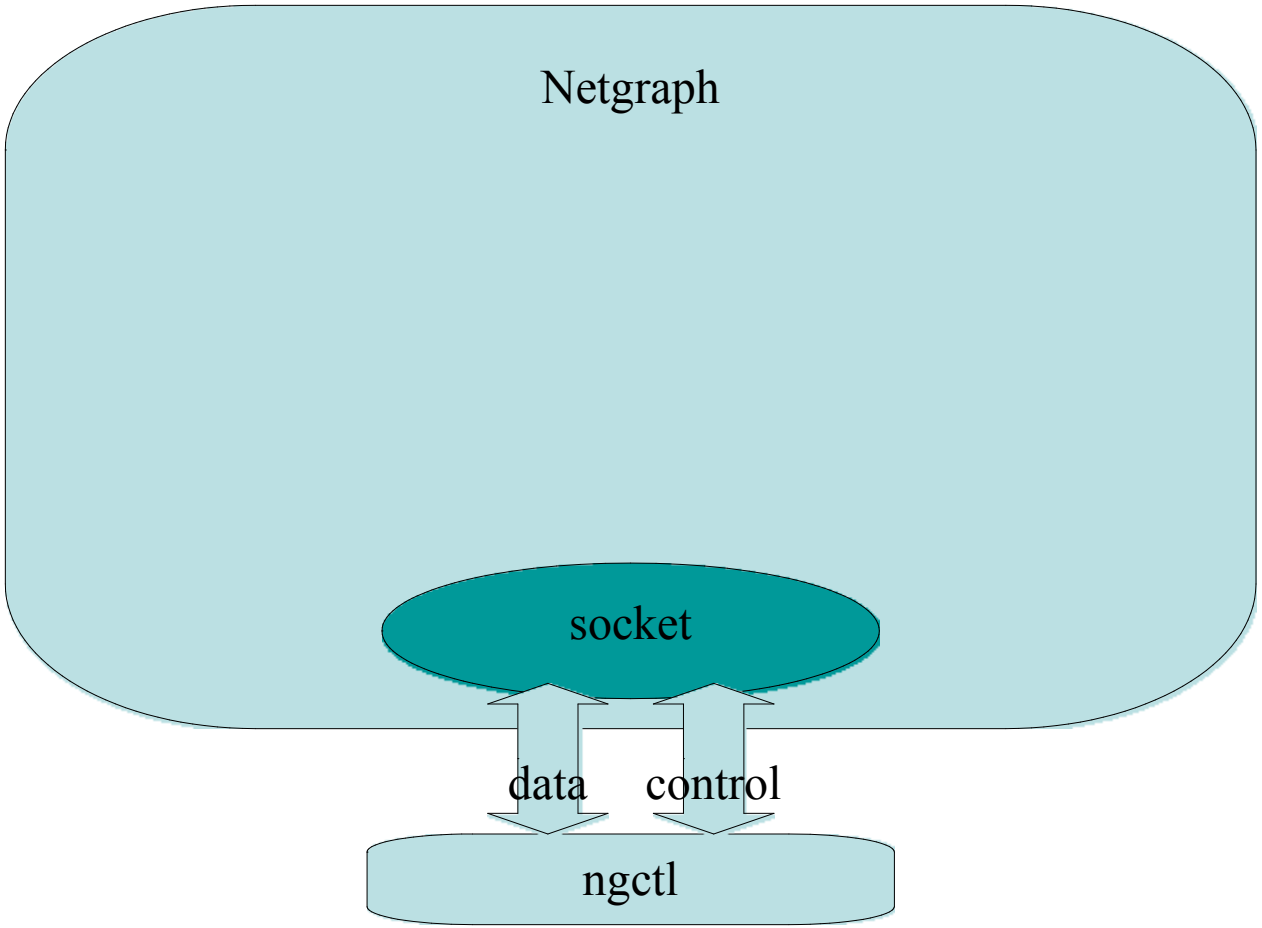
Netgraph

- Netgraph - это подсистема ядра для обработки пакетной информации, в первую очередь сетевого трафика.
- Netgraph отличают высокая гибкость и расширяемость и вместе с тем высокая производительность.
- Netgraph - это не конечный продукт для потребителя, но инструмент для разработчика и администриратора.

- В начале было слово, и было оно два байта и больше ничего не было...



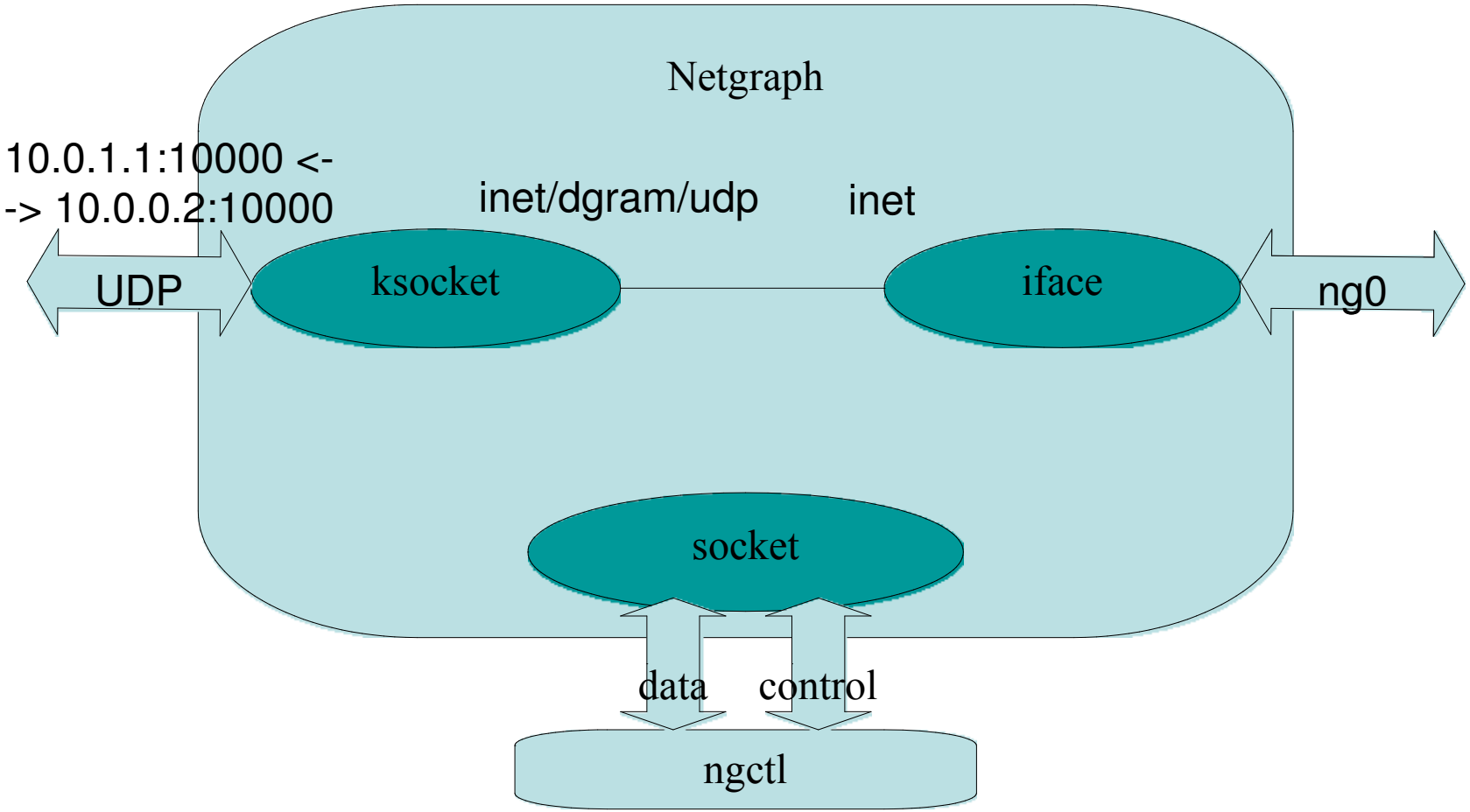
- Для взаимодействия с Netgraph служит модуль ng_socket и утилита ngctl.



- Вид на ноду socket глазами ngctl:

```
%ngctl list
There are 1 total nodes:
  Name: ngctl2171       Type: socket          ID: 00000005   Num hooks: 0
%
%
```

- Простейший UDP тунель с использованием модулей ng_iface и ng_ksocket.



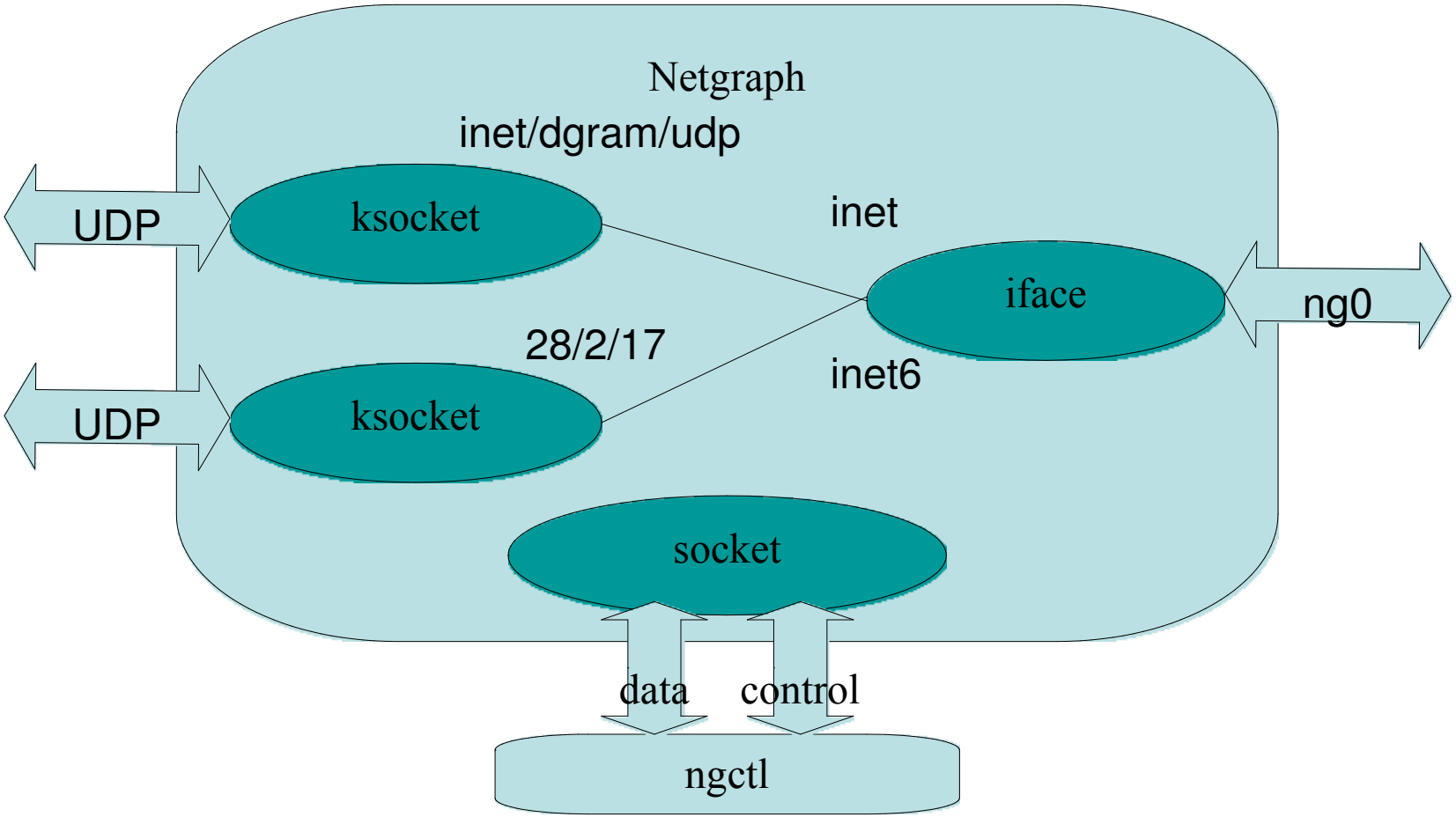
- то-же, но из командной строки:

```
%ngctl
Available commands:
  config     get or set configuration of node at <path>
  connect    Connects hook <peerhook> of the node at <relpath> to <hook>
  debug      Get/set debugging verbosity level
  dot        Produce a GraphViz (.dot) of the entire netgraph.
  help       Show command summary or get more help on a specific command
  list       Show information about all nodes
  mkpeer     Create and connect a new node to the node at "path"
  msg        Send a netgraph control message to the node at "path"
  name       Assign name <name> to the node at <path>
  read       Read and execute commands from a file
  rmhook     Disconnect hook "hook" of the node at "path"
  show       Show information about the node at <path>
  shutdown   Shutdown the node at <path>
  status     Get human readable status information from the node at <path>
  types      Show information about all installed node types
  write      Send a data packet down the hook named by "hook".
  quit       Exit program
+ mkpeer . iface qqq inet
+ rmhook . qqq
+ mkpeer ng0: ksocket inet inet/dgram/udp
+ name ng0:inet UDP
+ list
There are 7 total nodes:
  Name: ng0             Type: iface           ID: 00000008   Num hooks: 1
  Name: ngctl2228       Type: socket          ID: 00000007   Num hooks: 0
  Name: UDP             Type: ksocket         ID: 00000009   Num hooks: 1
+ show ng0:
  Name: ng0             Type: iface           ID: 00000008   Num hooks: 1
  Local hook      Peer name       Peer type    Peer ID         Peer hook
  ----------      ---------       ---------    -------         ---------
  inet            UDP             ksocket      00000009        inet/dgram/udp
+
```

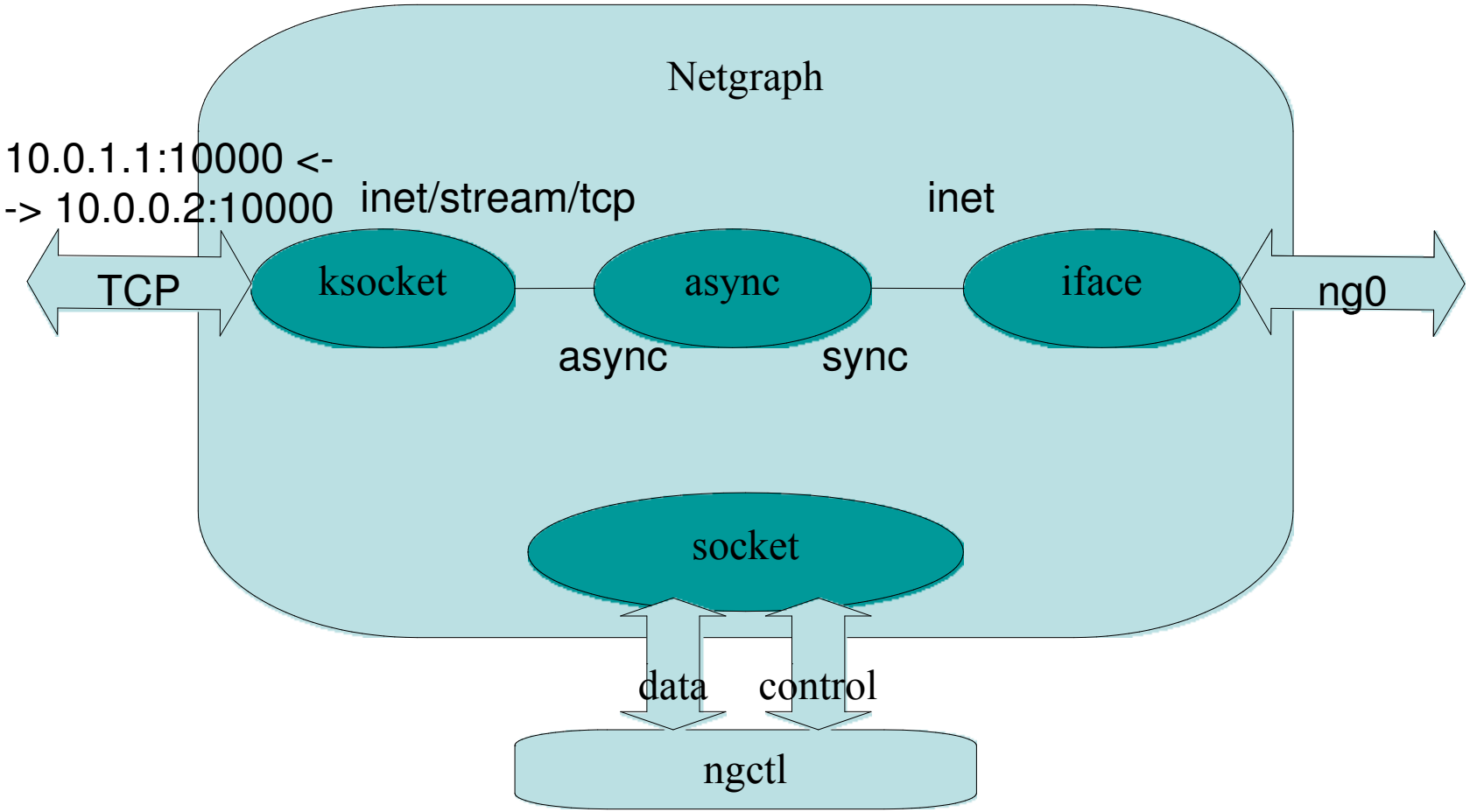
- осталось только установить соединение:

```
+ msg UDP: bind inet/10.0.0.2:10000
+ msg UDP: connect inet/10.0.1.1:10000
+ ^D
%netstat -an |grep 10000
udp4       0      0 10.0.0.2.10000         10.0.1.1.10000
%
```

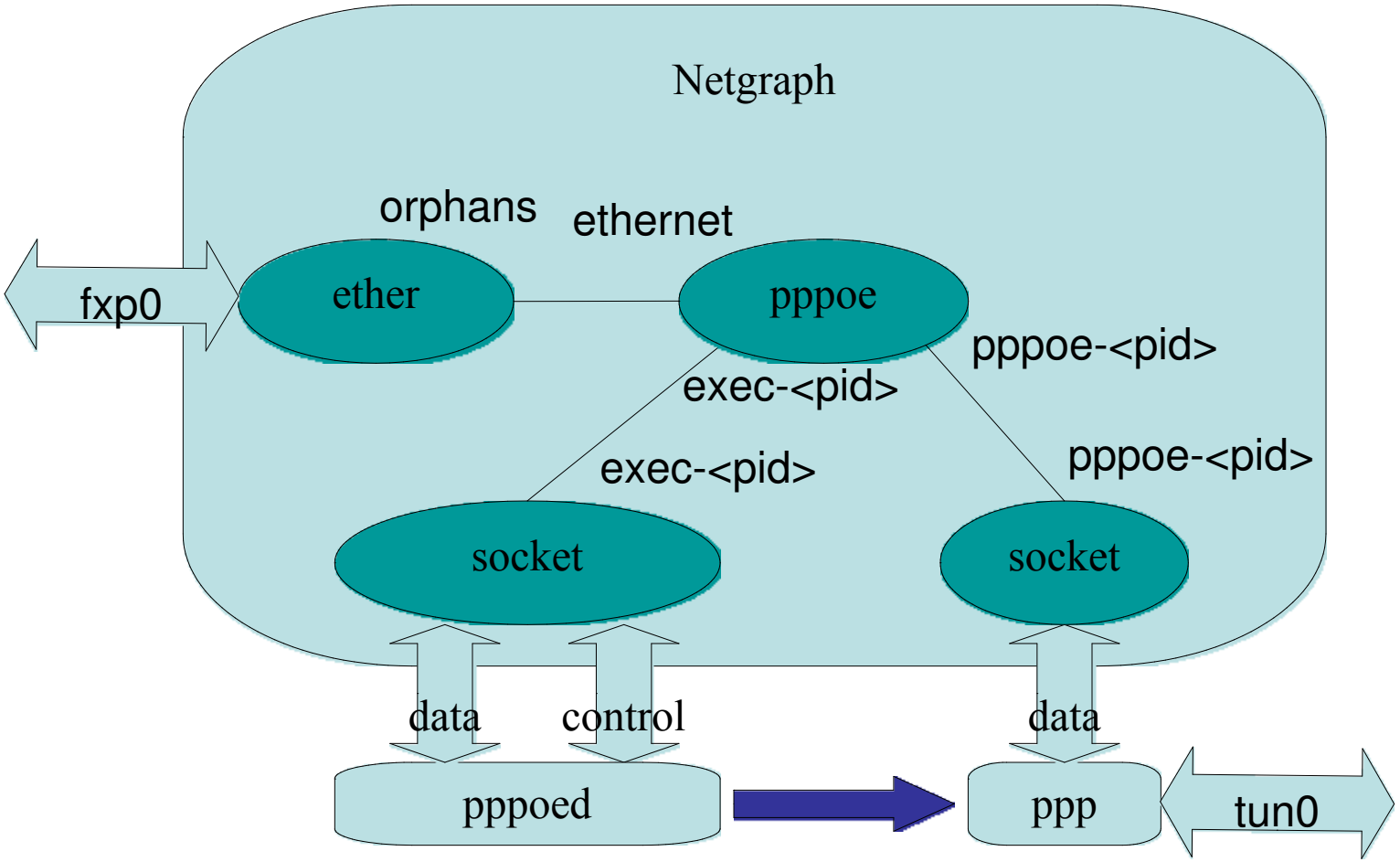
- Нужна так-же поддержка IPv6? Легко!



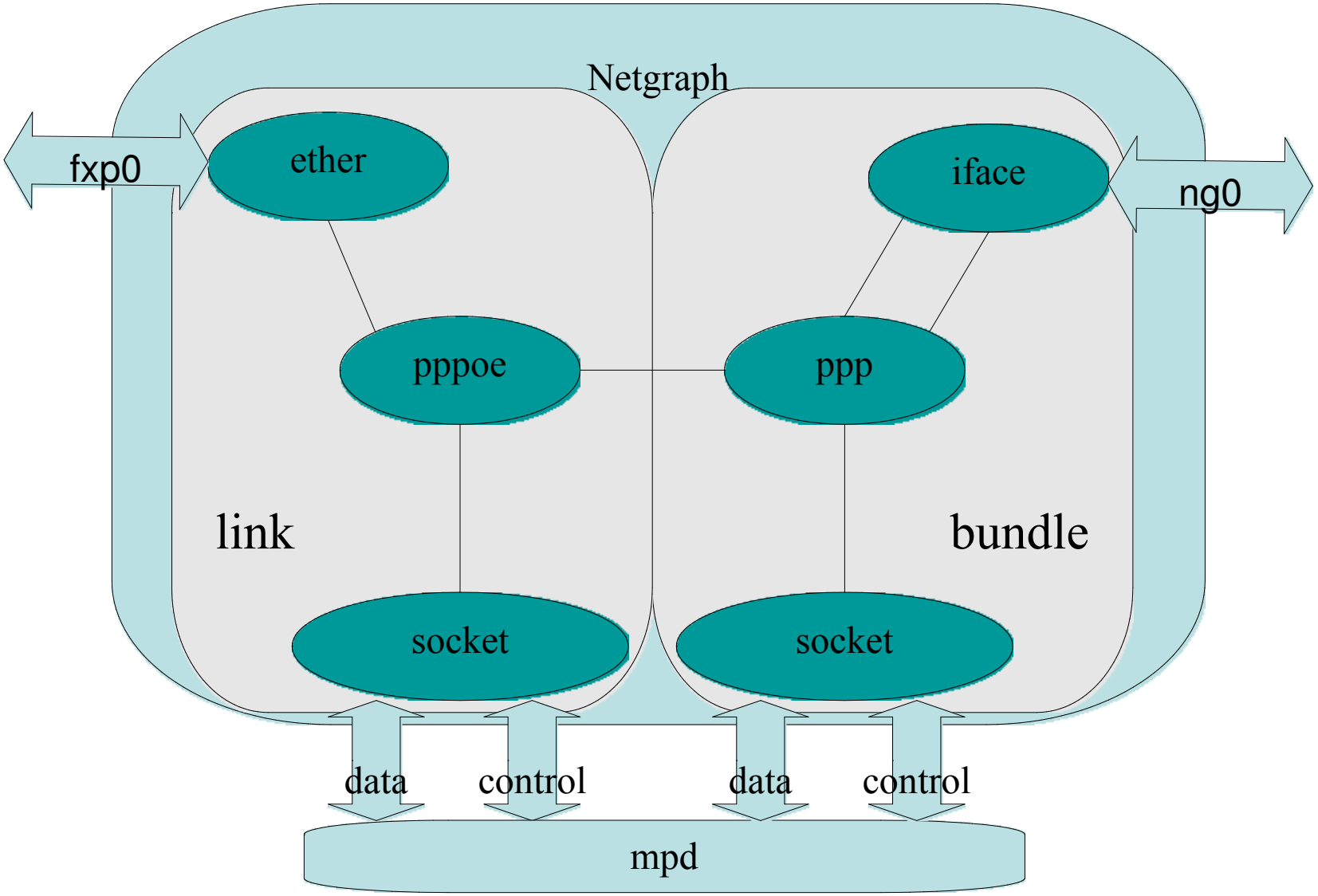
- А теперь немного сложнее - TCP тунель.



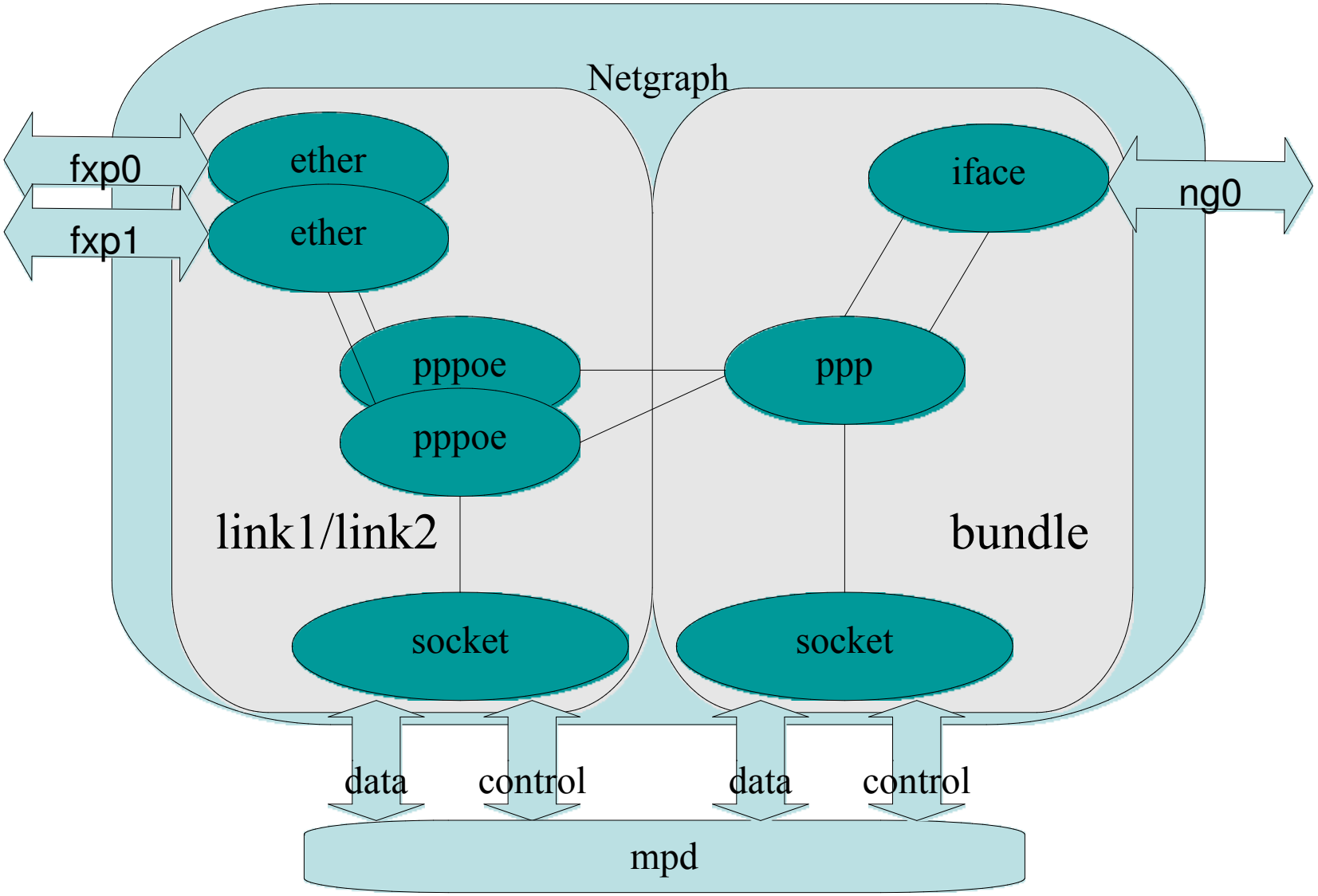
- pppoed - PPPoE сервер для «бедных». :)



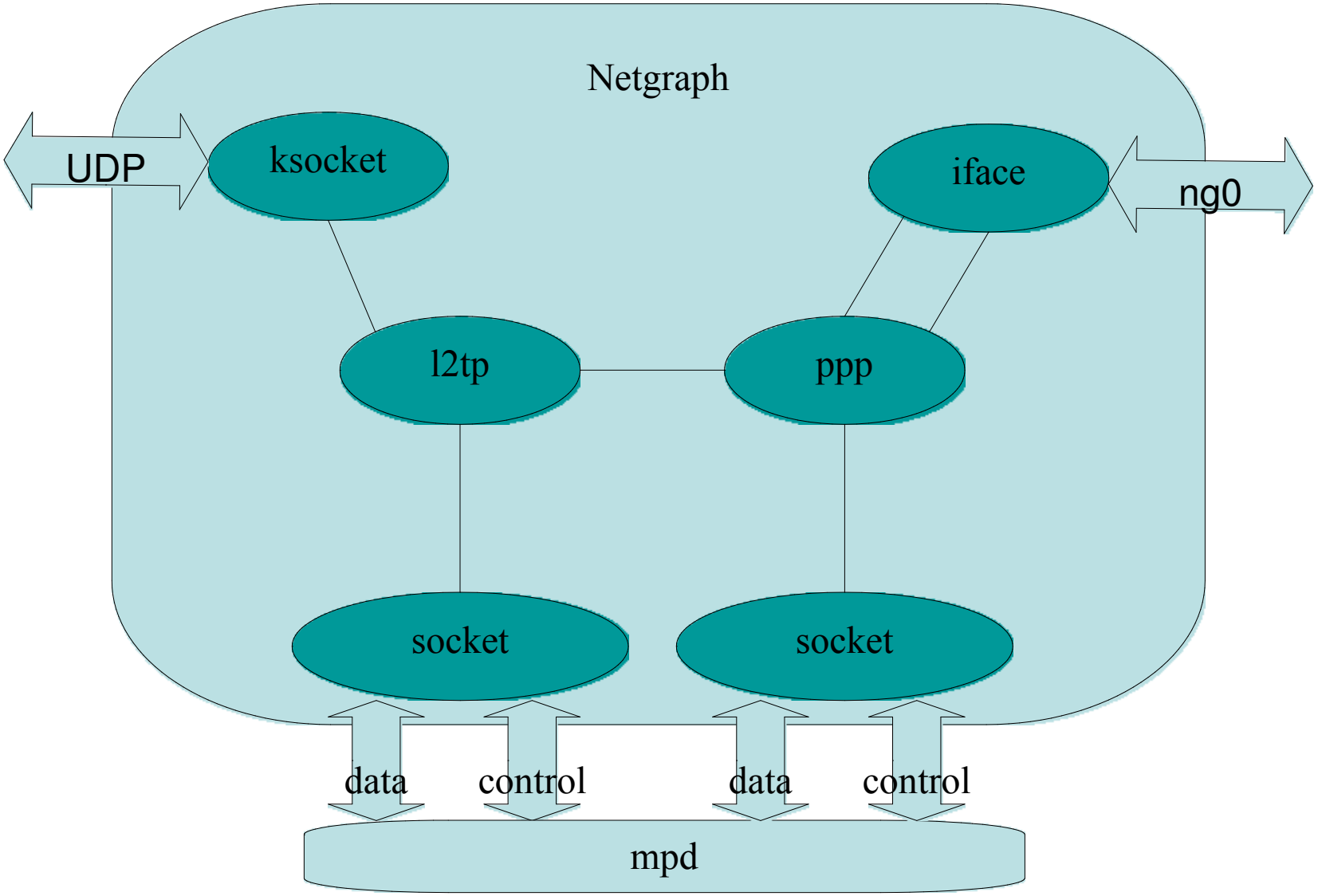
- mpd - PPP для взрослых. PPPoE.



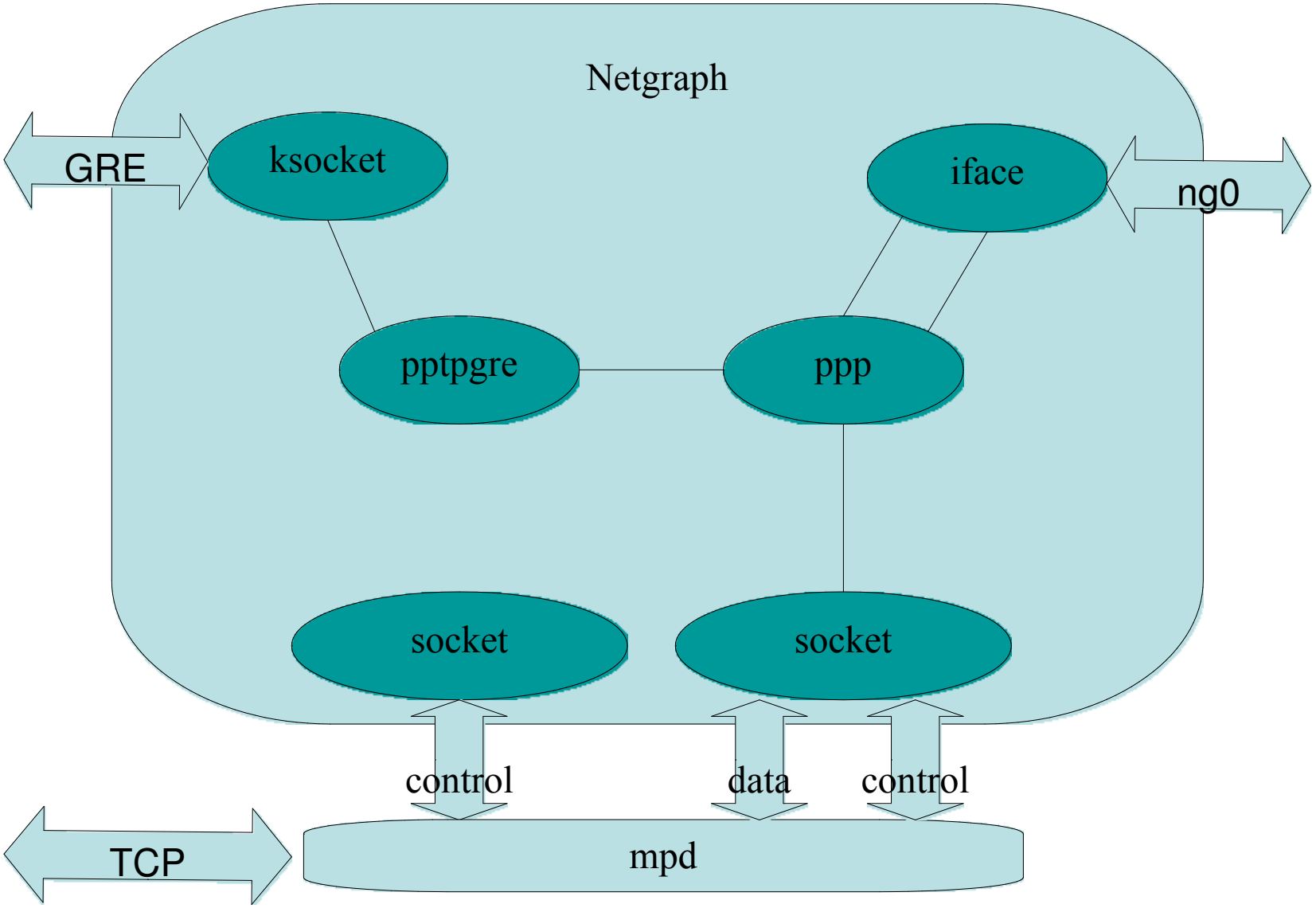
- mpd - PPP для взрослых. Multilink PPPoE.



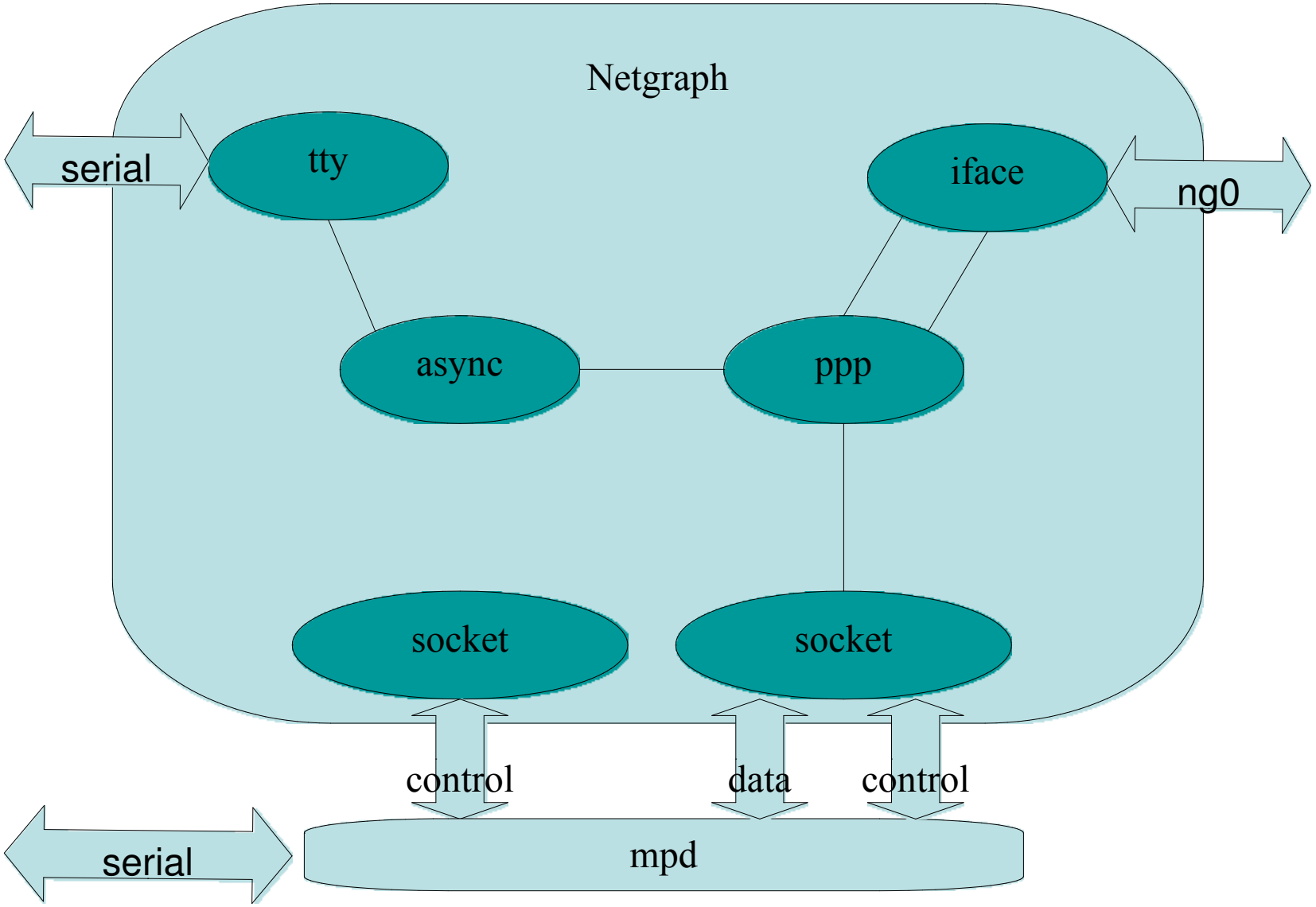
- mpd - PPP для взрослых. L2TP.



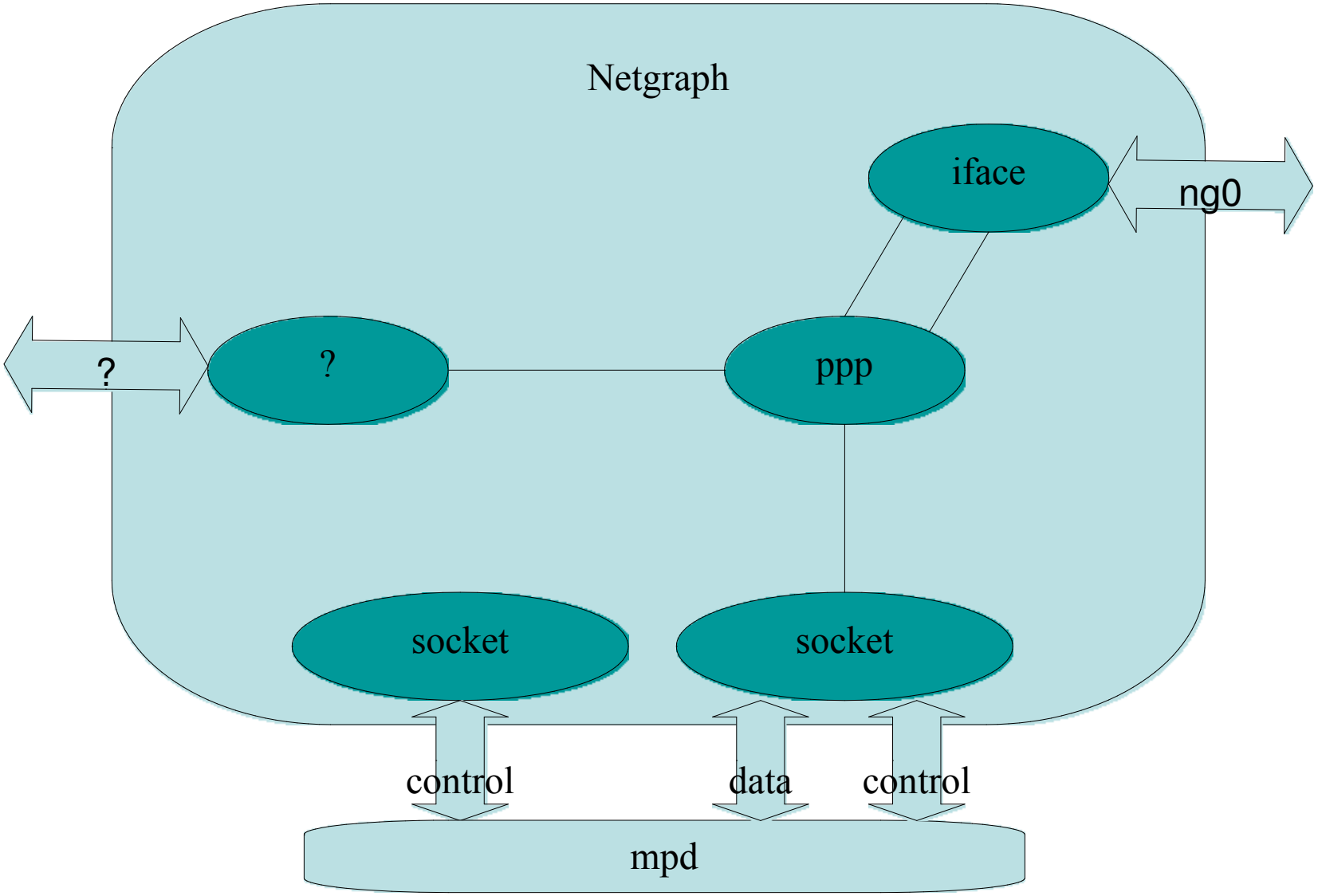
- mpd - PPP для взрослых. PPTP.



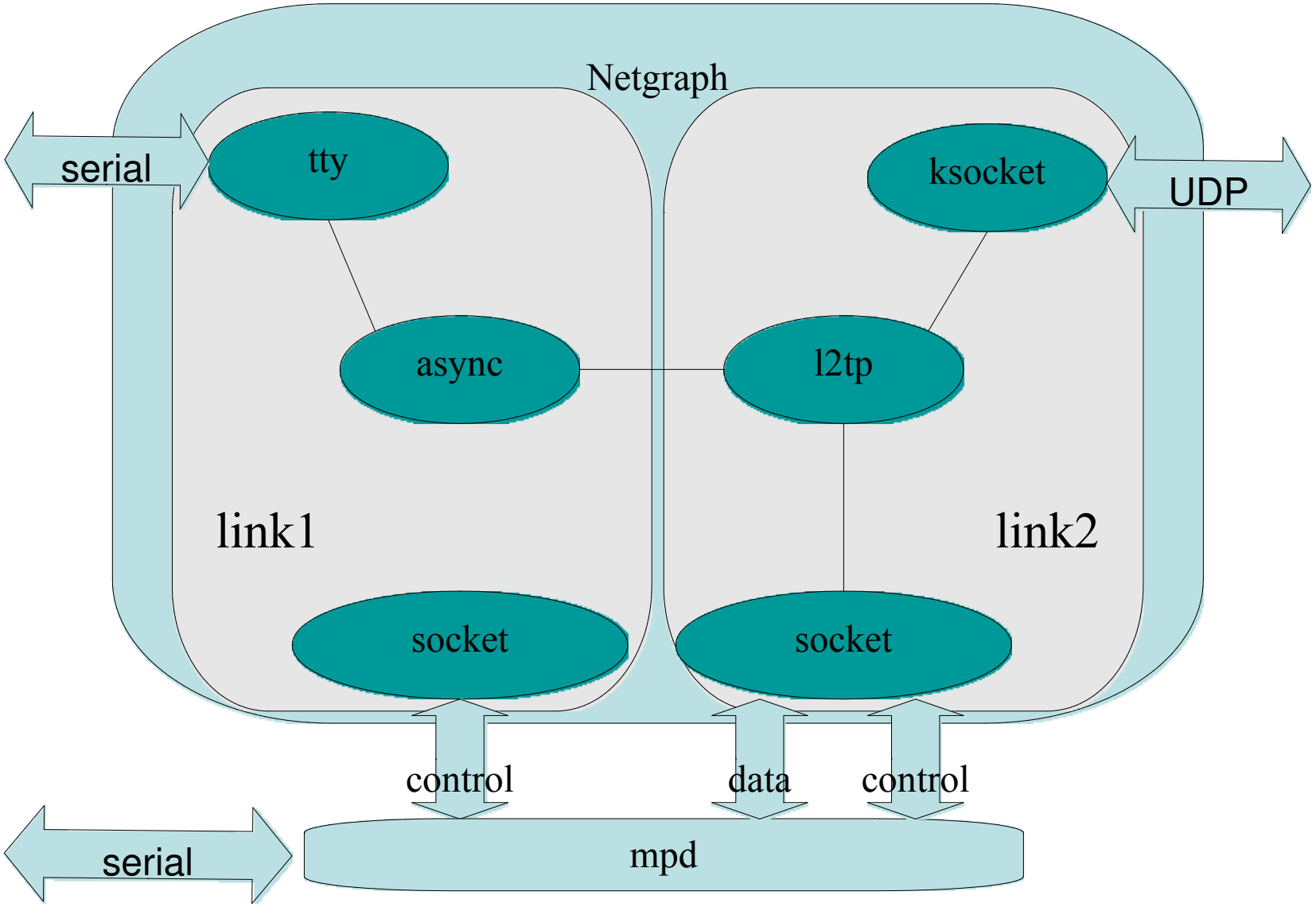
- mpd - PPP для взрослых. Modem.



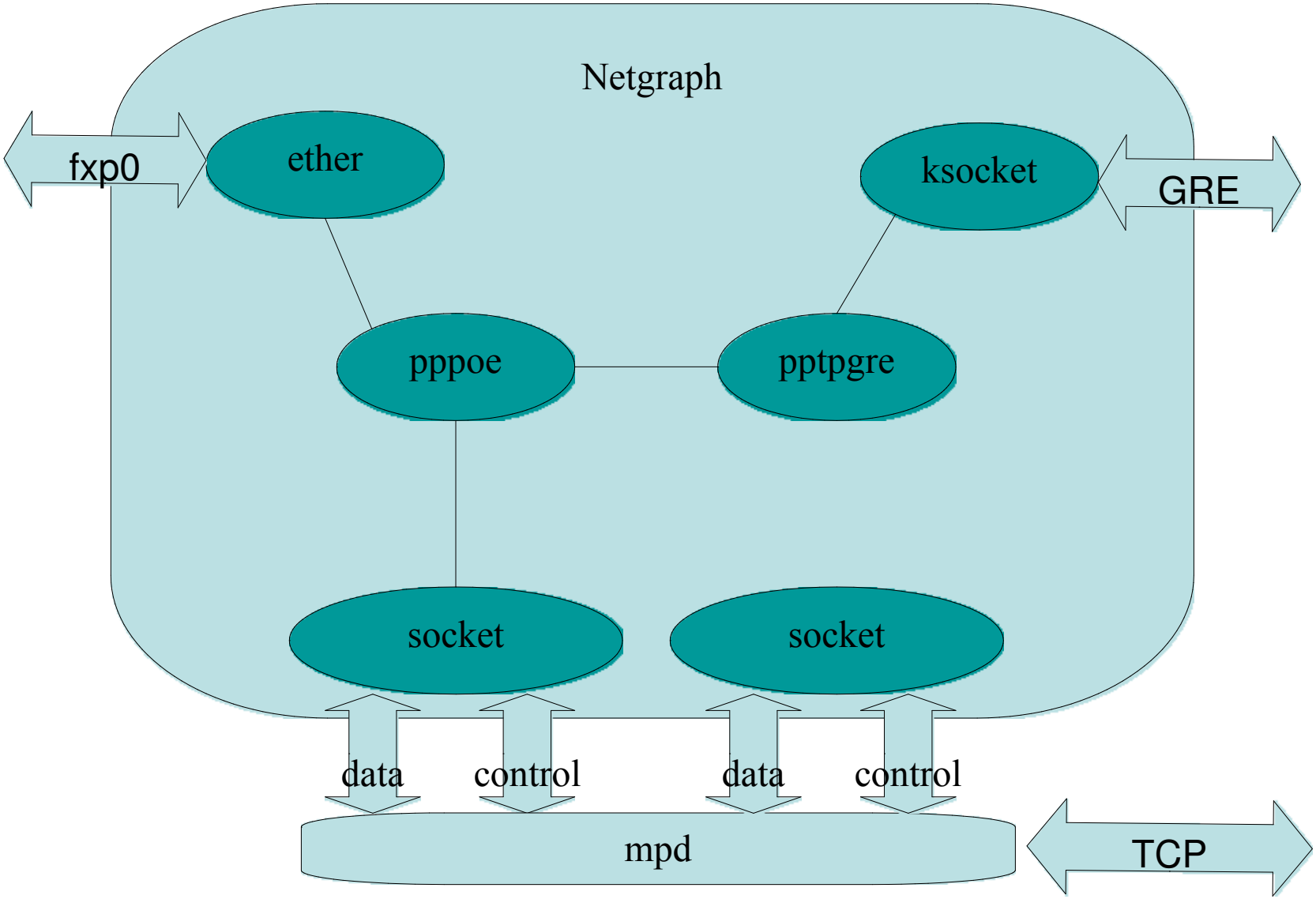
- ..., TCP, UDP, Sync, ... Чего еще изволите?



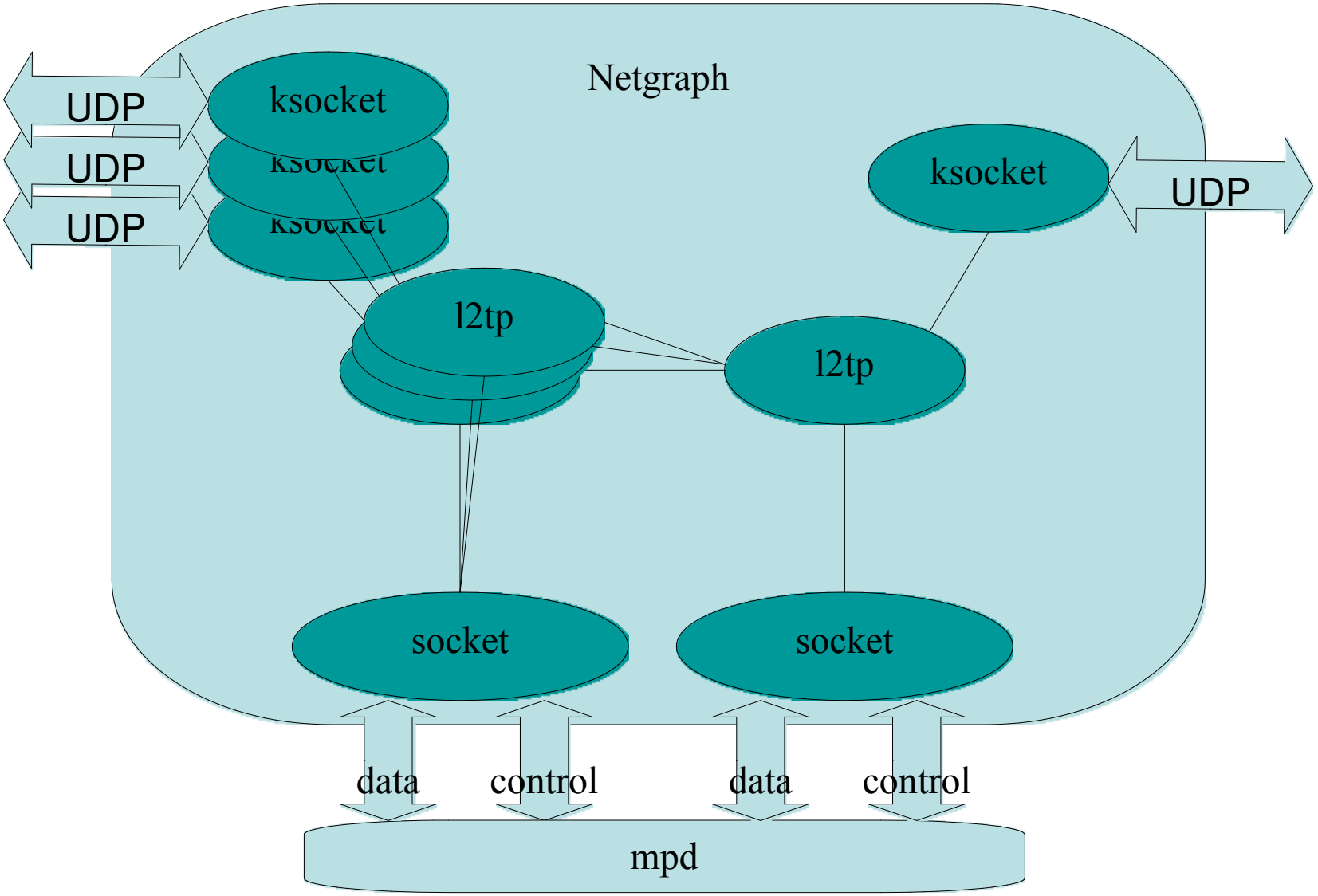
- LAC - L2TP Access Concentrator.



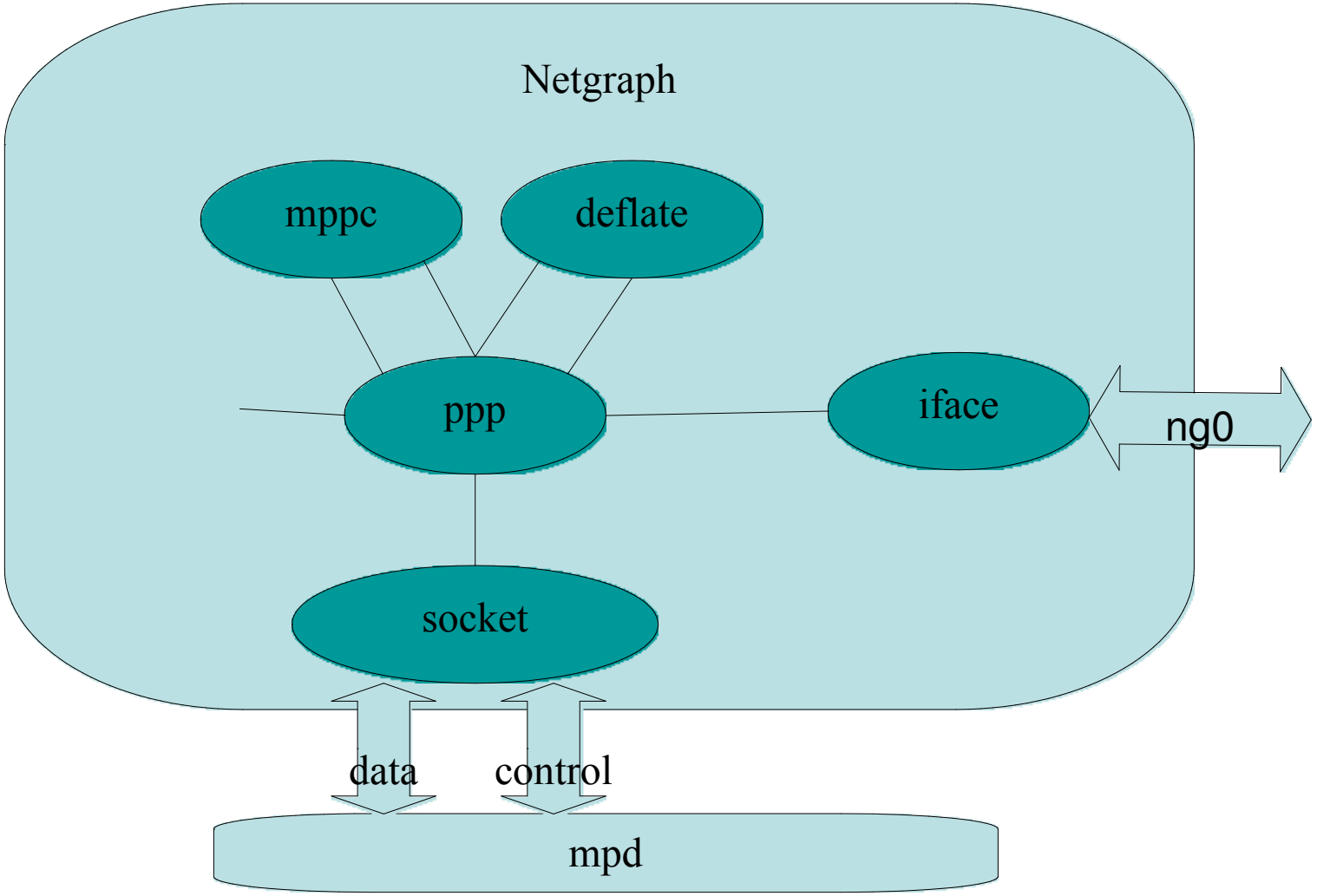
- PAC - PPTP Access Concentrator.



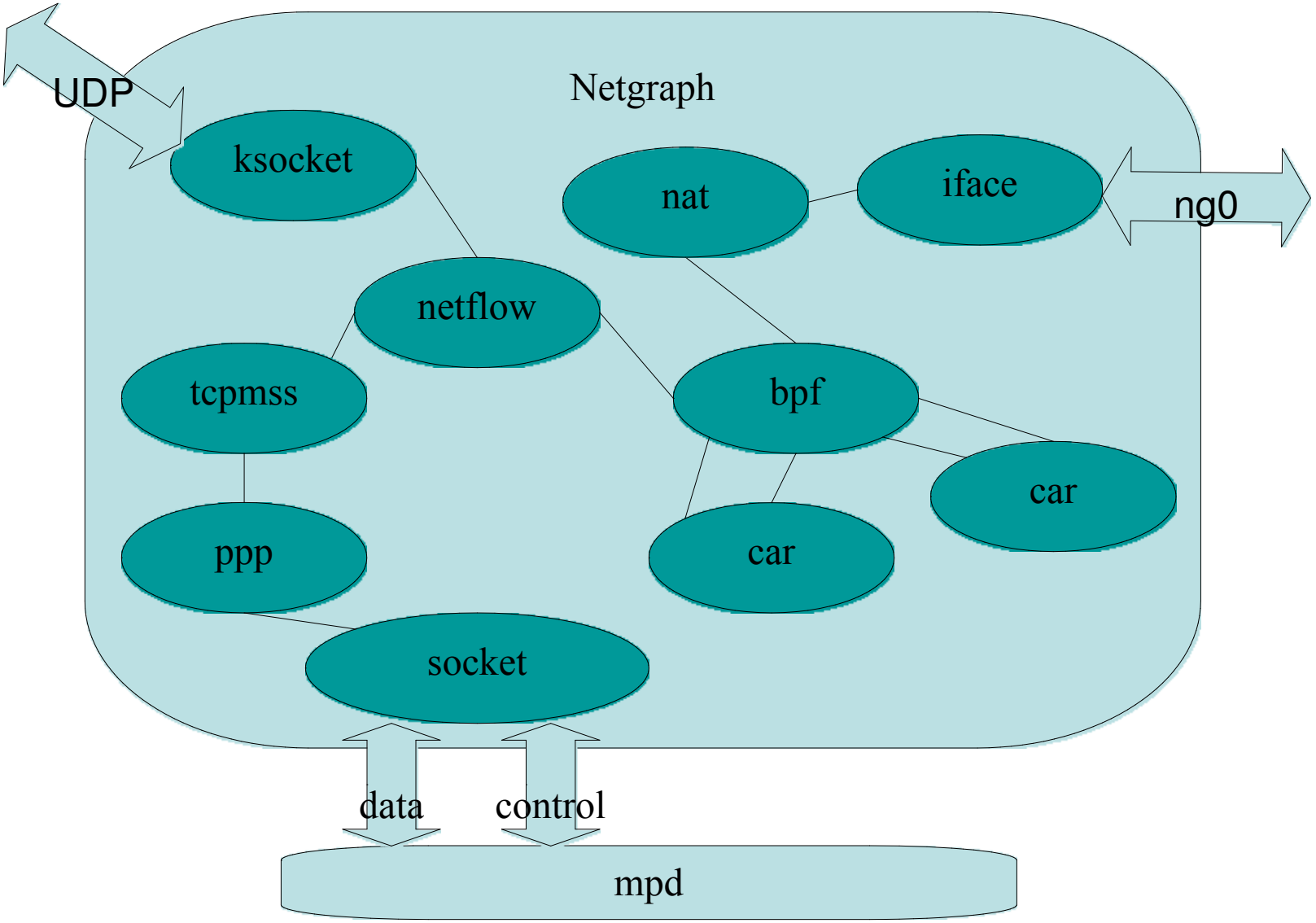
- TSA - Tunnel Switching Aggregator.



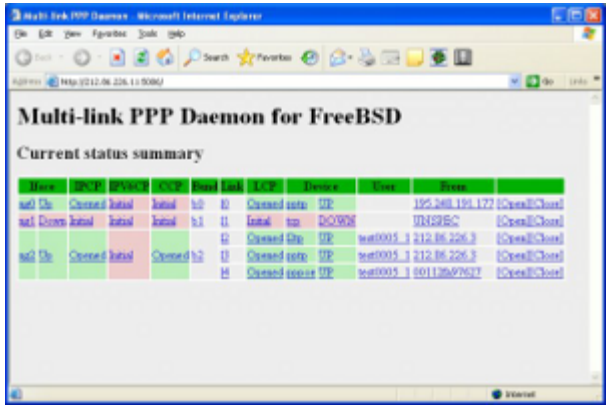
- Сжатие (VJC, MPPC, Deflate, Predictor-1), шифрование (MPPE, DESE)

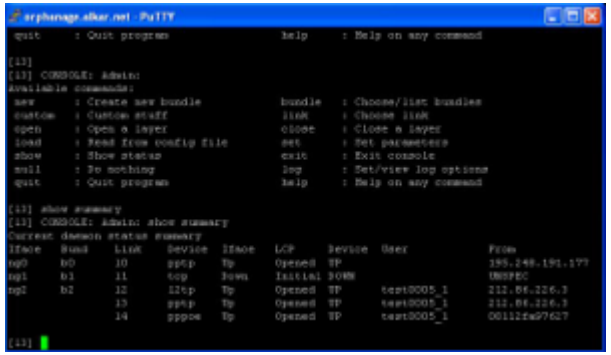


- Netflow, фильтры, шейпы, аккаунтинг, NAT



- Но не стоит забывать о user-level демоне:
  - управление netgraph,
  - внешнее взаимодействие:
    - консоль,
    - Telnet сервер,
    - HTTP сервер:
      - WEB интерфейс,
      - технический интерфейс (API),
    - RADIUS клиент и сервер,
  - файлы конфигурации,
  - язык управления модемом,
  - выдача IP адресов





- Но не стоит забывать о user-level демоне:
  - аутентификация:
    - PAP,
    - CHAP,
    - MS-CHAPv1,
    - MS-CHAPv2,
    - EAP,
  - авторизация и аккаунтинг:
    - internal (файл с паролями),
    - system (passwd/utmp/wtmp),
    - PAM,
    - external (вызов внешних скриптов),
    - RADIUS,

- Но не стоит забывать о user-level демоне:
  - динамическая авторизация:
    - обрыв сессии:
      - Telnet консоль
      - WEB-интерфейс
      - RADIUS-client аккаунтинг
      - RADIUS-server Disconnect-Request
    - изменение параметров сессии «на лету»:
      - RADIUS-server Change of Authorization (CoA)
  - управление ограничением и подсчетом трафика.

- Ну и конечно производительность!
  На Core2Duo 2.4GHz с 512MB (менее $1000 даже в серверном исполнении) под FreeBSD 7.2, mpd5.3, oops и quagga одновременно обслуживаются:
  - 2500 PPPoE сессий,
  - 500Mbit/s трафика,
  - до 100 новых подключений в секунду,
  - поклиентные фильтры/классификаторы трафика,
  - поклиентные шейпы для каждого фильтра,
  - RADIUS аккаунтинг поклиентно по типам трафика каждые 2.5 минуты,
  - генерация Netflow,
  - режим мягкого отключения (captive portal),
  - ...