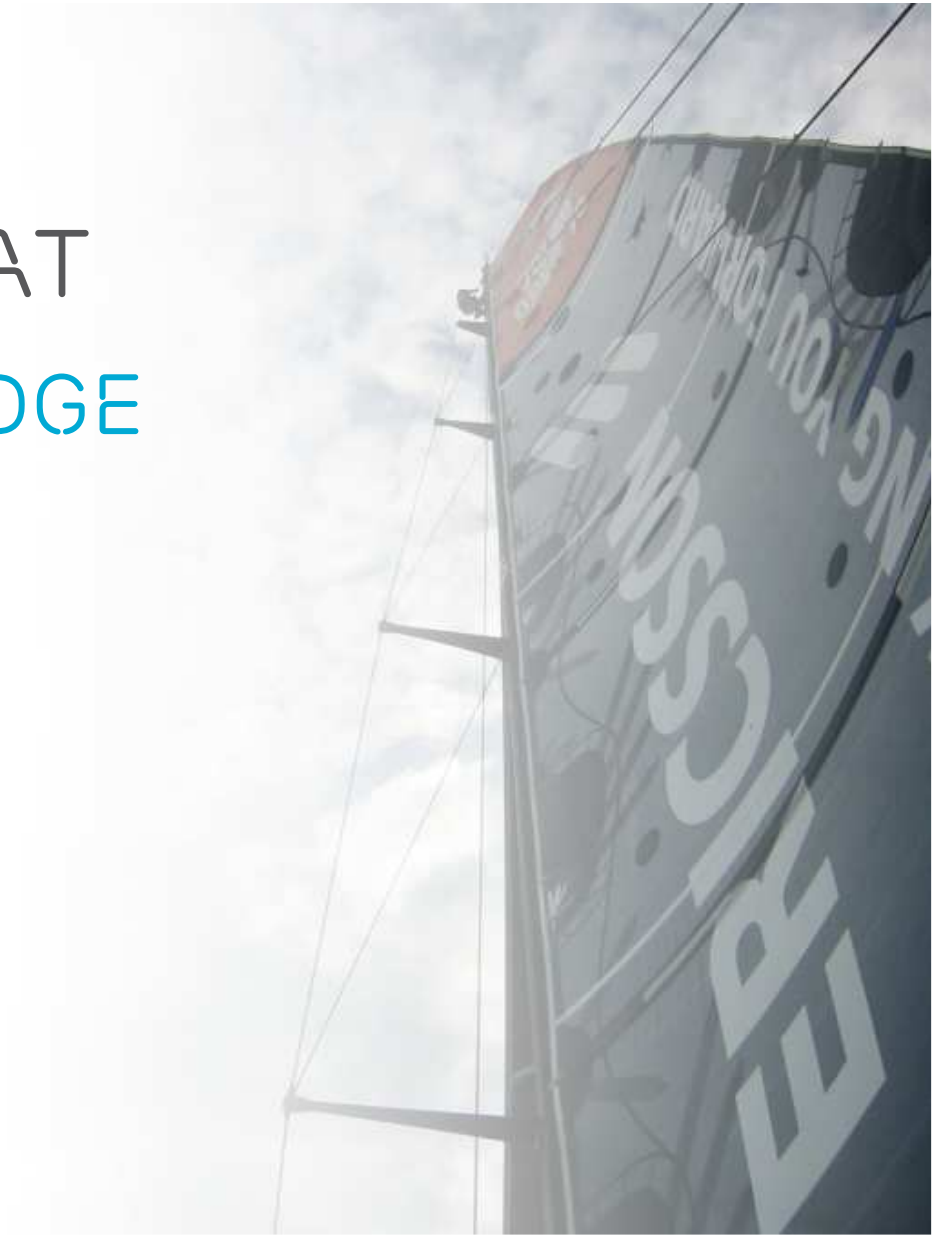
CARRIER-GRADE NAT

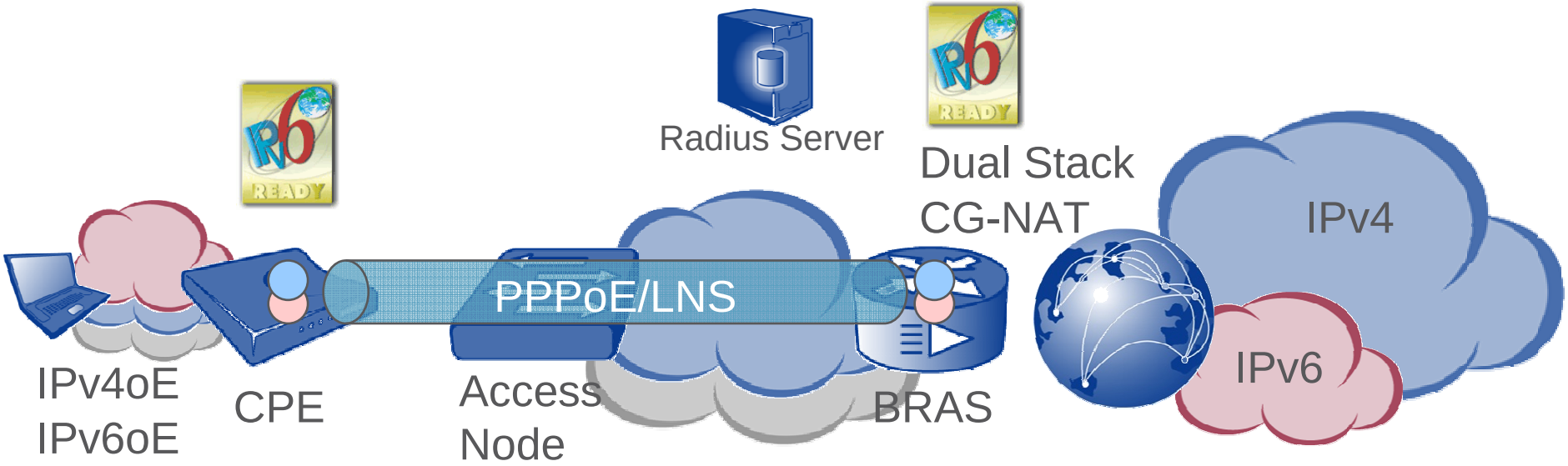
B ERICSSON SMARTEDGE



СОДЕРЖАНИЕ

ПЕРЕХОД К IPV6

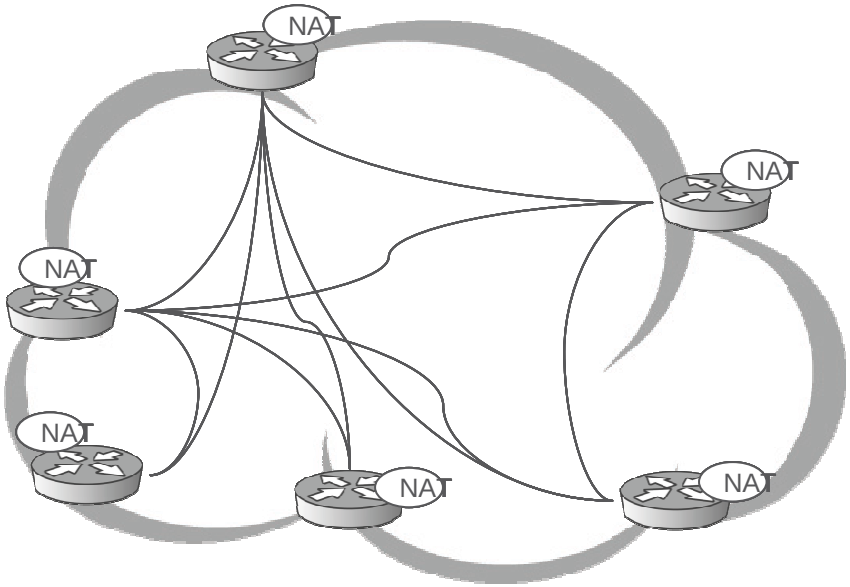
DUAL-STACK + NAT444



- Поддержка IPv6 требуется от CPE, если CPE работает в режиме router, в случае если bridge – то не требуется
- BRAS использует Dual Stack для каждого абонента, в случае полного исчерпания v4 пространства, для стека v4 включается функция NAT44 (Carrier Grade)
- Поддержка IPv6 от инфраструктуры доступа и метро агрегации не требуется
- Каждый стек управляем со стороны AAA

ОПТИМАЛЬНЫЙ ДИЗАЙН NAT

РАСПРЕДЕЛЁННАЯ МОДЕЛЬ, ИНТЕГРИРОВАННЫЙ CG-NAT



- Нет влияния на путь прохождения трафика
- Управление NAT политикой со стороны AAA
- Отсутствие дополнительной точки отказа в виде NAT фермы
- Обработка трафика без дополнительных специализированных устройств

СОДЕРЖАНИЕ

ЧТО ТАКОЕ CG-NAT В SMARTEDGE?

- Поддержка с SEOS 11.1
- Лицензируемая функция
  - Наличие лицензии обязательно
  - Без лицензии конфигурация недоступна
- Поддержка RFC: 4787 (UDP), 5382 (TCP) 5508 (ICMP), draft-nishitani-cgn
- Поддержка Address Pairing (soft and hard limit)
- Поддержка logging/tracing
- Поддержка всех типов абонентов(PPPoE,CLIPS,LNS)
  - Для LNS поддерживается только CG-NAT
- Поддержка Full Cone NAT для UDP и TCP
- Трансляция фрагментированных пакетов.
- Поддержка UDP Refresh
- Поддержка ICMP Notifications
- Количество трансляций
  - PPA2/3, SE100 – 2M активных трансляций на модуль
  - Количество трансляций фиксировано

СОДЕРЖАНИЕ

CGNAT – АКТИВАЦИЯ ЛИЦЕНЗИИ

- Legacy NAT -> без лицензии
- CGNAT -> необходима лицензия

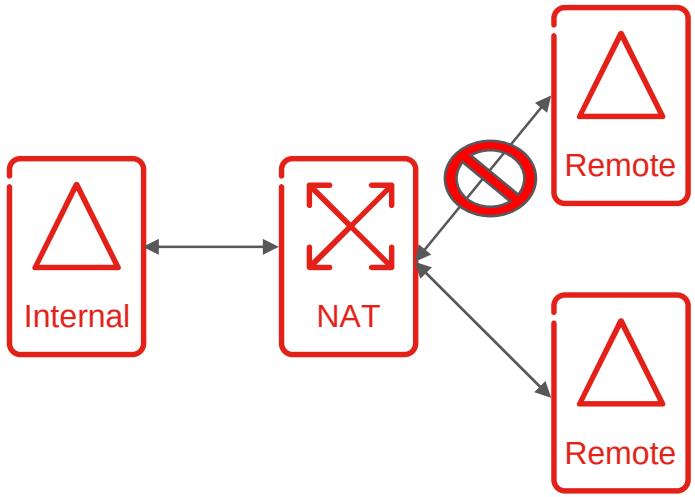
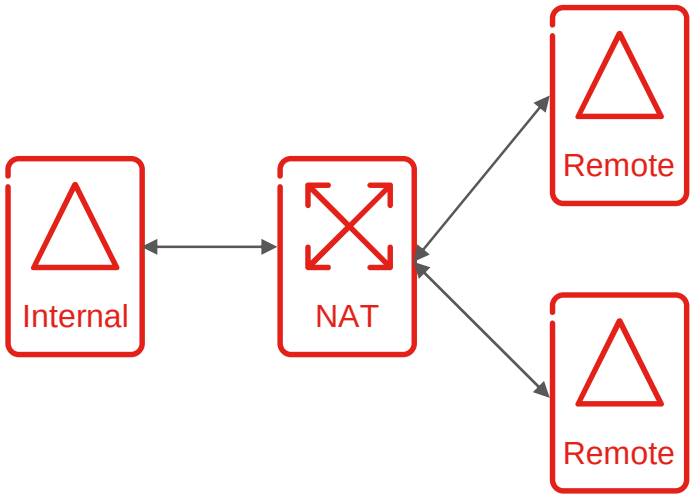
- Активация лицензии:
- software license
- nat enhanced encrypted 1 …

CGNAT – СОЗДАНИЕ ПОЛИТИКИ

- Legacy NAT -> без enhanced
- CGNAT -> keyword enhanced

- Создание политики:
- nat policy basic_nat **enhanced**
- ...
- Ключевое слово в CLI для создания CG-NAT политики - enhanced

CGNAT – POINT TO MULTIPOINT SESSIONS FOR TCP OVERVIEW

Point to point One internal –one remote endpoint	Point to multipoint One internal – more remote endpoint
	

НАСТРОЙКА CGNAT – POINT TO MULTIPOINT SESSIONS FOR TCP

```
context nat_context
nat policy basic_nat enhanced
! Default class
  drop
! Named classes
  access-group basic_nat_rules
   class yes_p2mp
    pool NAPT_POOL local
     endpoint-independent filtering udp
     endpoint-independent filtering tcp
     timeout abandoned 1800
```

CGNAT – ТРАНСЛЯЦИЯ ФРАГМЕНТИРОВАННЫХ ПАКЕТОВ

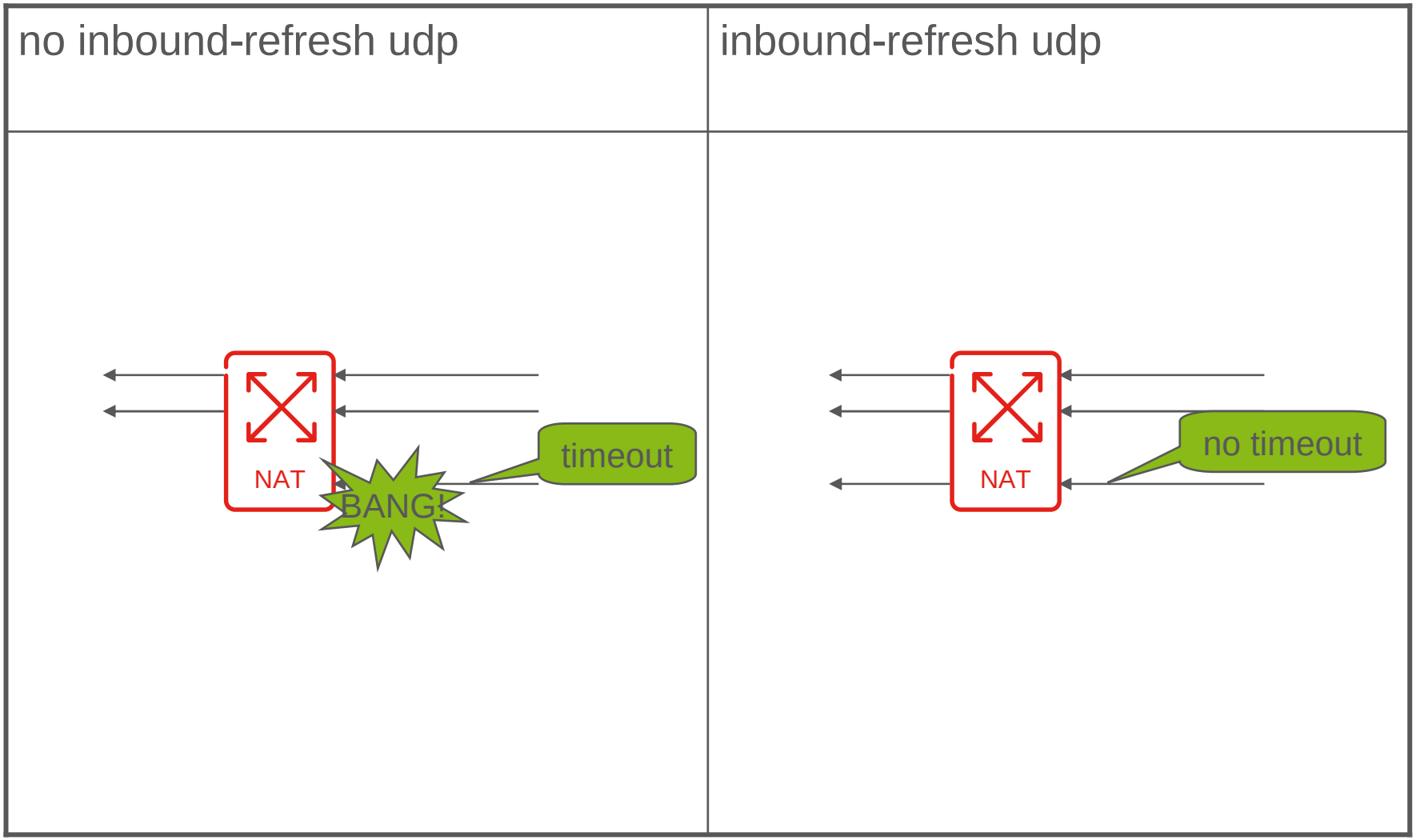
- Legacy NAT -> фрагментированные пакеты уничтожаются (<0.2%)
- CGNAT -> фрагментированные пакеты транслируются

- Поддержка TCP,UDP,ICMP(за исключением ICMP Error)
- Минимальная длина пакета – 220 Байт(включая заголовок)

- Условия включения:
  - В контексте отсутствует сконфигурированный NAT пул с блоками портов.
  - В контексте отсуствует NAT политика привязанная к абоненту.
  - В контексте отсуствует NAT пул привязанный к политике.
- Условия отключения:
  - В контексте отсуствует NAT политика привязанная к абоненту.
  - В контексте отсуствует NAT пул привязанный к политике.

- Настройка на контекст:
- context local
- [no] nat fragments

CGNAT – INBOUND REFRESH BEHAVIOR FOR UDP OVERVIEW



НАСТРОЙКА CGNAT - INBOUND REFRESH BEHAVIOR

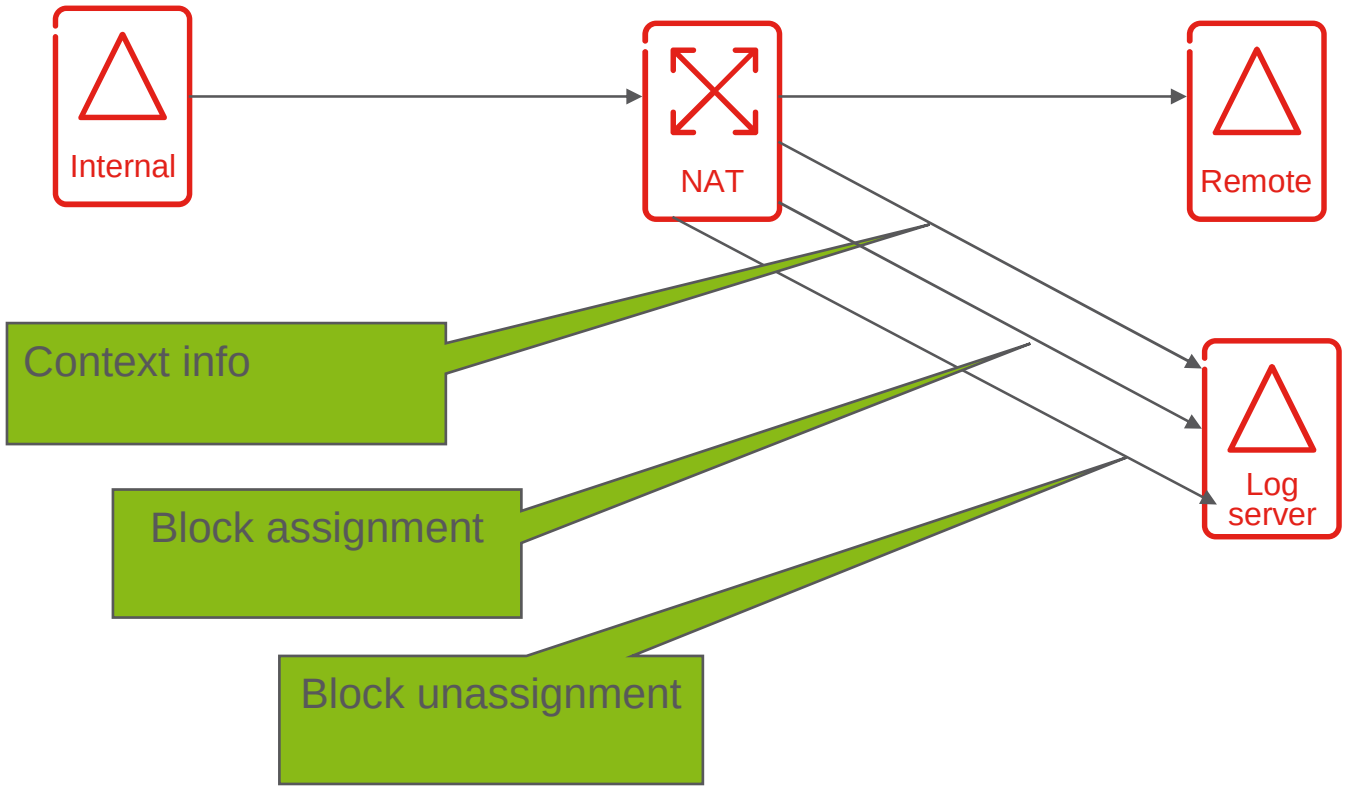
- *no inbound-refresh udp*
- *inbound-refresh udp*

CGNAT - БЛОКИ ПОРТОВ С ДИАПАЗОНАМИ IP АДРЕСОВ

- Legacy NAT -> 1 IP с блоком портов
- Enhanced CGNAT -> Диапазон адресов с блоками портов

- Настройка диапазона адресов с блоками портов:
- context nat_context
- ip nat pool NAPT_POOL napt multibind
- address 10.10.10.1 to 10.10.10.99 port-block 1 to 15

CGNAT – ОБЗОР ЛОГГИРОВАНИЯ



CGNAT - ОБЗОР ЛОГГИРОВАНИЯ

Содержание сообщения в коллектор:

Context Info

CONTEXT_ID

CONTEXT_NAME

Block Assignment

CONTEXT_ID

ASSIGN_TS_SEC

IPV4_INT_ADDR

IPV4_EXT_ADDR

EXT_PORT_FIRST

EXT_PORT_LAST

Block Un-assignment

CONTEXT_ID

ASSIGN_TS_SEC

UNASSIGN_TS_SEC

IPV4_INT_ADDR

IPV4_EXT_ADDR

EXT_PORT_FIRST

EXT_PORT_LAST

CGNAT – ОБЗОР ЛОГИРОВАНИЯ

Логгируемые поля:

Field Type	Value	Length (bytes)	Description
CONTEXT_ID	24628	4	Internal context ID
CONTEXT_NAME	24629	64	Zero terminated context Name
ASSIGN_TS_SEC	24630	4	Seconds of UNIX timestamp for assign
UNASSIGN_TS_SEC	24631	4	Seconds of UNIX timestamp for unassign
IPV4_INT_ADDR	24632	4	Internal IPv4 address
IPV4_EXT_ADDR	24633	4	External IPv4 address
EXT_PORT_FIRST	24634	2	External L4 port start
EXT_PORT_LAST	24635	2	External L4 port end

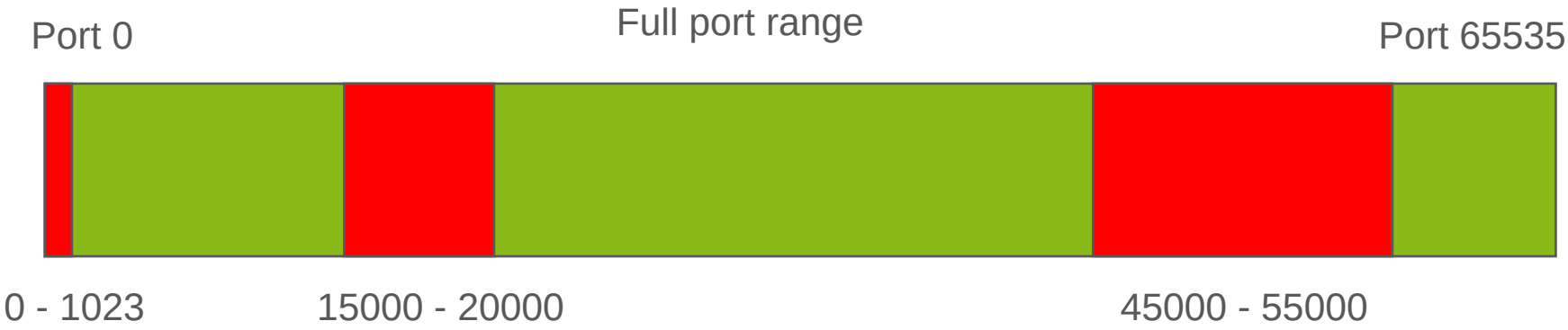
НАСТРОЙКА CGNAT - ЛОГГИРОВАНИЕ АЛЛОКАЦИЙ

- context local
  nat logging-profile nat-log-profile1
- context nat-context
  nat logging-profile nat-log-profile2
  transport-protocol udp
  export-version v9
  source-ip-address 10.10.10.1
  source-port 4242
  destination-ip-address 100.1.1.1 context local
  destination-port 8989
  dscp ef
  maximum ip-packet-size 1400
- ip nat pool nat-pool napt multibind logging
  logging-profile nat-log-profile1 context local
  logging-profile nat-log-profile2

USEFUL OPERATIONAL COMMANDS

- show nat profile
- show nat pool
- show card x nat ctxinfo
- show card x nat profile
- show card x nat pool

CGNAT – ИСКЛЮЧЕНИЕ ПОРТОВ ИЗ ПУЛА



Available ranges

Excluded port ranges

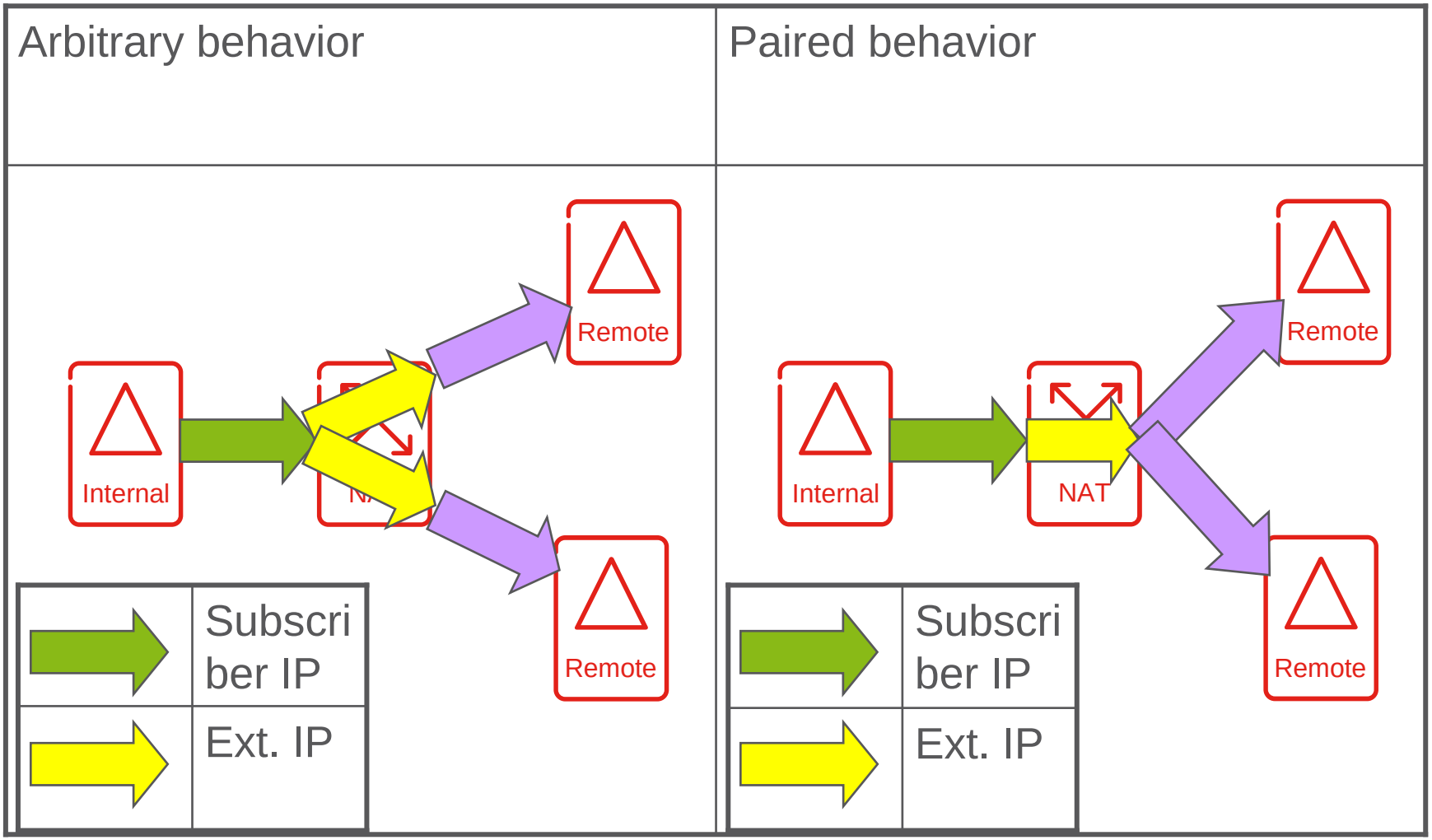
HOW TO CONFIGURE CGNAT - EXCLUDE PORT RANGES FROM POOL

- context nat_context
- ip nat pool nat-pool napt multibind
- address 85.62.163.1 to 85.62.163.14
- exclude well-known
- exclude 15000 to 20000
- exclude 45000 to 55000

USEFUL OPERATIONAL COMMANDS

- show nat pool
- show card x nat pool

CGNAT – ADDRESS PAIRING



НАСТРОЙКА CGNAT – ADDRESS PAIRING

- *ip nat pool poolname napt **paired***
- *paired-mode subscriber over-subscription <users-per-IP> [port-limit <limit>]*
- or
- *paired-mode subscriber [over-subscription <users-per-IP>] port-limit <limit>*

over-subscription – мягкое ограничение количества внутренних адресов на один внешний адрес, без ограничения трансляций на адрес.

port-limit – жесткое ограничение количества трансляций на один адрес(без привязки к протоколу)

НАСТРОЙКА CGNAT - PAIRED BEHAVIOR

- **Пример 1 – 64 пользователя делят один внешний адрес**
- context nat_context
- ip nat pool nat-pool-paired napt paired
- paired-mode subscriber over-subscription 64
- address 100.100.100.1/32
- nat policy pol-nat enhanced
- ! Default class
- pool nat-pool-paired local

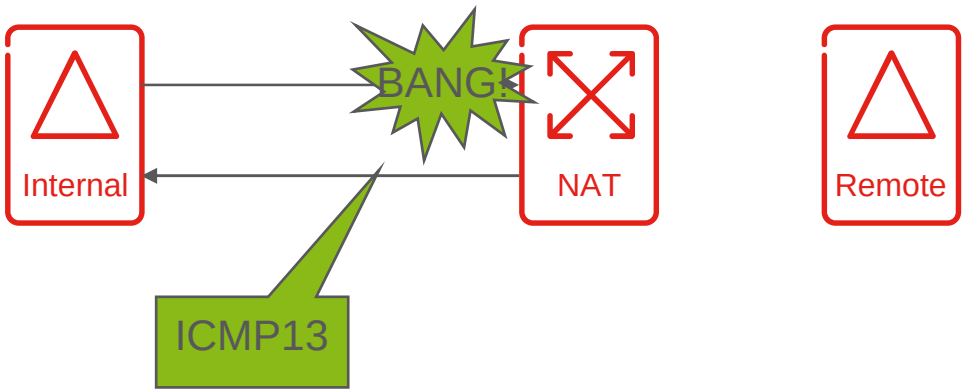
НАСТРОЙКА CGNAT - PAIRED BEHAVIOR

- **Пример 2, жесткое ограничение количества трансляций на пользователя**
- context nat_context
- ip nat pool nat-pool-paired napt paired
- paired-mode subscriber port-limit 1024
- address 100.100.100.1/32
- address 100.100.100.2/32
- nat policy pol-nat enhanced
- ! Default class
- pool nat-pool-paired local

НАСТРОЙКА CGNAT - PAIRED BEHAVIOR

- **Пример 3, комбинирование мягкого и жесткого ограничений на пользователей – 32 пользователя на 1 внешний адрес с ограничением количества трансляций(портов) 4096 на пользователя**
- context nat_context
- ip nat pool nat-pool-paired napt paired
- paired-mode subscriber over-subscription 32 port-limit 4096
- address 100.100.100.1/24
- nat policy pol-nat enhanced
- ! Default class
- pool nat-pool-paired local

CGNAT – ICMP NOTIFICATION



› В случае невозможности создания трансляции по тем или иным причинам внутреннему хосту посылается ICMP type 2 code 13 (Communication Administratively Prohibited)

НАСТРОЙКА CGNAT – ICMP NOTIFICATON

- nat policy pol-nat enhanced
- ! Default class
- no icmp-notification

КОНФИГУРАЦИЯ CG-NAT

```
context local
nat logging-profile DEFAULT_NAT_LOGGING
  transport-protocol udp
  source 10.6.19.37 port 5000
  destination 10.14.33.50 context local port 5000
  dscp ef
context local
ip nat pool RESIDENTIAL_6K_PORTS napt paired-mode logging
  paired-mode subscriber over-subscription 10 port-limit 6000
  logging-profile DEFAULT_NAT_LOGGING context local
  address 87.0.0.1 to 87.0.0.254
   exclude well-known
context local
 nat policy RESIDENTIAL_6K_PORTS enhanced
pool RESIDENTIAL_6K_PORTS local
  inbound-refresh udp
  icmp-notification
end
```

СОДЕРЖАНИЕ

УТИЛИЗАЦИЯ NAT

- [local]Redback#show card 2 nat allocation

- Slot 2, Ingress:
- Microblock counters:
- used count : 1885
- unassigned count : 9603
- free count : 54048
- [local]Redback#

- 1 микроблок = 32 порта = 32 **возможных** трансляции
- Количество трансляций ~= (used count)*32

- used count = количество микроблоков использованных и алоцированных к circuits

- unassigned count = количество микроблоков которые уже преалоцированы в память PPA, но не используются circuits и могут быть быстро присвоены при необходимости.

- free count = оставшееся количество свободных микроблоков.


ERICSSON