

Skoltech

Skolkovo Institute of Science and Technology



Lomonosov Moscow
State University

NETCONF/YANG

Лекция 7

Василий Пашков

`pashkov@lvk.cs.msu.su`



SNMP vs NETCONF

SNMP



- SNMP = Simple Network Management Protocol
- Управление сетевыми устройствами
- Прикладной уровень по модели OSI/ISO
- Транспорт: UDP, порты: 161, 162
- 1988 – 1991 г. – SNMPv1
- SNMPv2
- SNMPv3 с криптографической защитой (порты 10161, 10162)

Недостатки SNMP



- Транспортный протокол UDP => возможны потери (и даже подмены)
- Можно записывать/считывать только одно определенное значение за один раз. Нельзя послать несколько значений в одной транзакции
- Нет возможности откатов/бэкапов конфигурации
- Ограничения в SMI (например, длины некоторых полей)
- Зоопарк MIB даже у одного вендора, даже в одном типе устройств



- NETCONF – Network Configuration Protocol
- Протокол управления конфигурацией сетевых устройств
- IETF NETCONF Working Group
- 2006 г – **RFC4741**
 - <http://tools.ietf.org/html/rfc4741>
- 2011 г – **RFC6241**
 - <http://tools.ietf.org/html/rfc6241>
- Juniper (на основе Junos XML API)

NETCONF vs SNMP



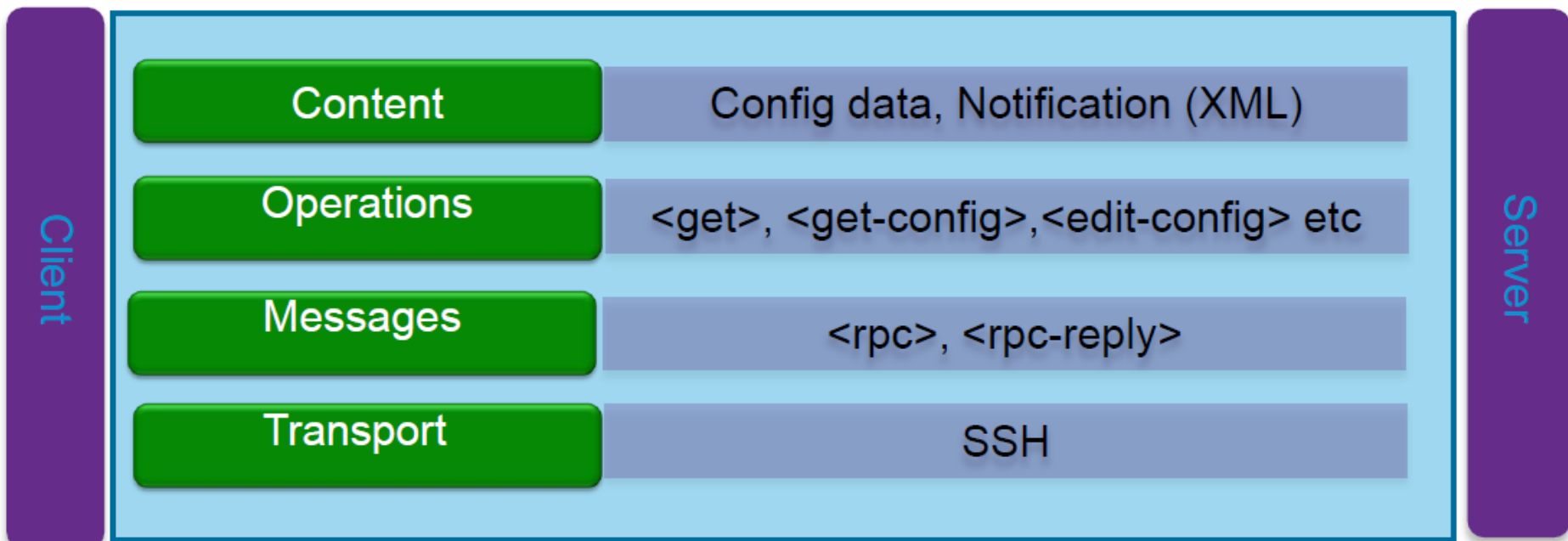
Сценарий	SNMP	NETCONF
Получение группы параметров о состоянии	Да	Да. Гораздо быстрее, чем SNMP
Изменение группы параметров	Да, до 64kB	Да
Транзакционное изменение параметров	Нет	Да
Транзакция через группу сетевых устройств	Нет	Да
Вызов административных функций	Теоретически	Да
Отсылка уведомление	Да	Да
Резервное копирование и восстановление	Обычно нет	Да
Защищенный протокол	V3	Да
Тестирование конфигурации перед применением	Нет	Да

Набор поддерживаемых сценариев делают NETCONF более привлекательным!



NETCONF

Уровни в NETCONF



- Клиент-серверная модель (сервером выступает сетевое устройство)
- Поддержка соединения - Установленную сессию можно держать сколько угодно долго

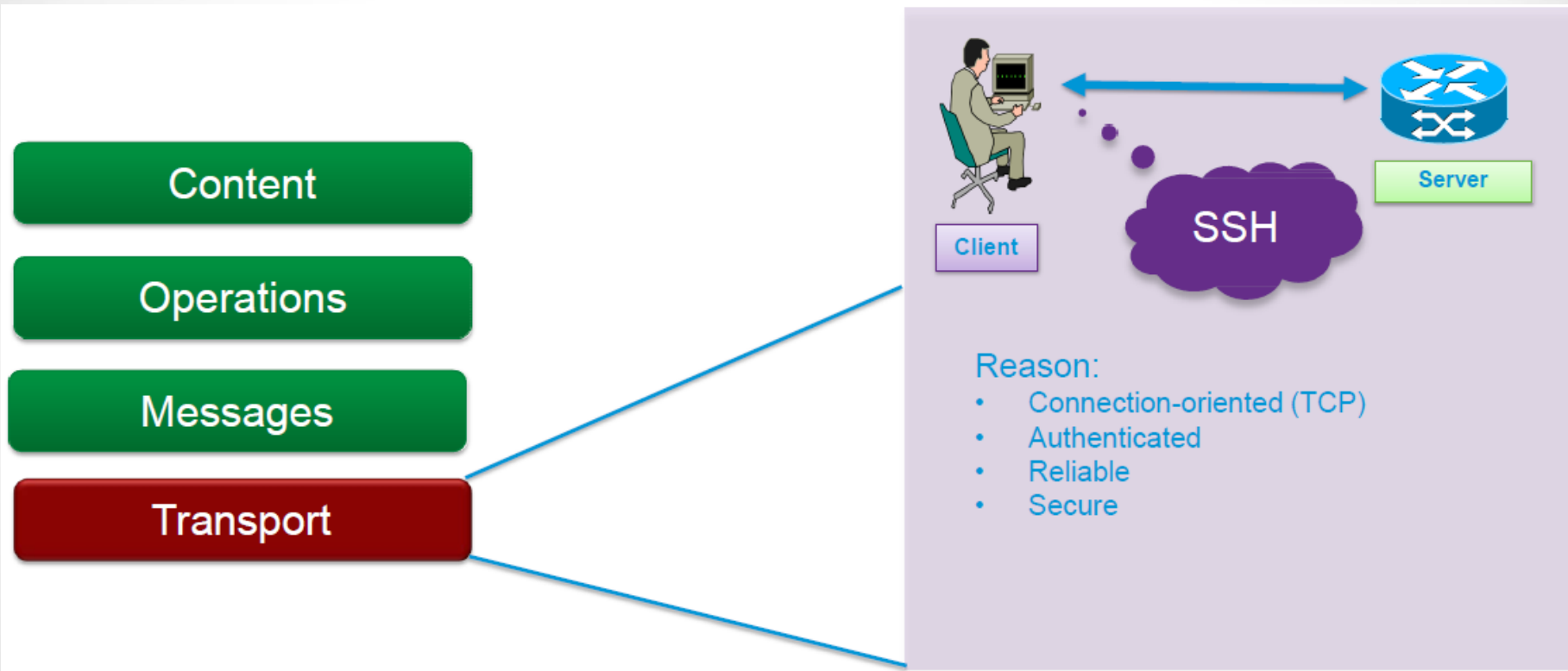
IETF стандарты NETCONF



V 1.0	V 1.1	Extension
RFC 6535 Background and Requirements	RFC 6241 1.1 Base NETCONF Protocol	RFC 5277 Notifications
RFC 4741 1.0 Base NETCONF Protocol	RFC 6242 NETCONF over SSH	RFC 5717 Partial Locking
RFC 4742 NETCONF over SSH		RFC 6243 With defaults
		RFC 6244 NETCONF + YANG Architectural Overview

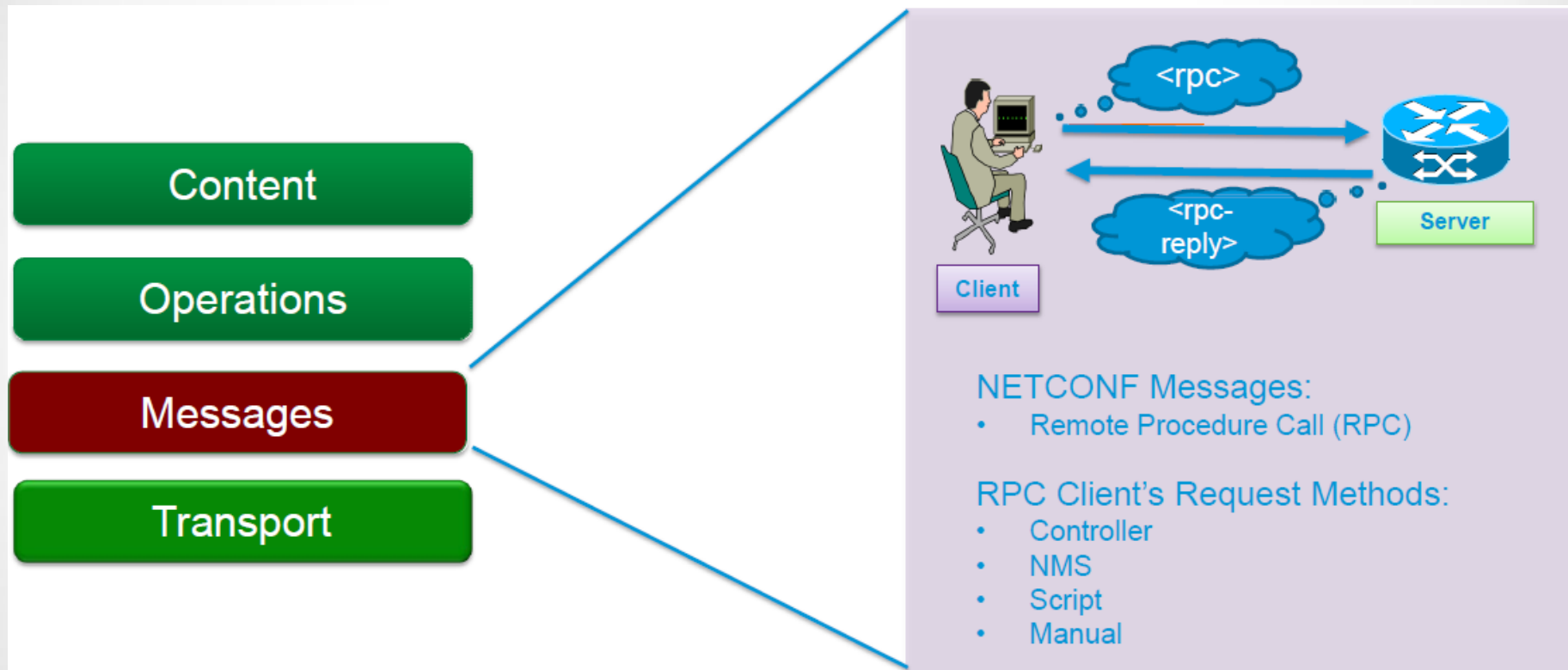


NETCONF протокол (1)





NETCONF протокол (2)





NETCONF протокол (3)

Content

Operations

Messages

Transport

OPERATION	DESCRIPTION
<get-config>	Retrieve data from the running configuration
<get>	Retrieve running configuration or device statistic
<edit-config>	Modify a configuration database - operation = merge (default), delete, create, replace, remove - test-option (:validate), error-option
<copy-config>	Copy a configuration database
<delete-config>	Delete a configuration database
<commit>	Commit candidate configuration to the running db
<lock>/<unlock>	Lock or unlock a configuration datastore system
<close-session>	Terminate this session
<kill-session>	Force Termination of session

NETCONF протокол (4)



Content

Operations

Messages

Transport

```
<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
      urn:ietf:params:netconf:base:1.0
    </capability>
    <capability>
      urn:ietf:params:netconf:capability:candidate:1.0
    </capability>
    <capability>
      urn:ietf:params:netconf:capability:notification:1.0
    </capability>
  </capabilities>
  <session-id>285212672</session-id>
</hello>
]]>]]>
```

Возможности NETCONF



- Открывать несколько сессий
- Работать с разными конфигурациями (например: `running` или `startup`)
- Запрашивать конфигурацию и состояние одним запросом с поиском
- Производить конфигурацию нескольких параметров одним запросом
- Получать результаты операций в виде ответов (`rpc-reply`)
- Делать `commit` и `rollback` (применение и откат конфигураций)



YANG

Yet Another Next Generation



- Язык моделирования данных YANG был разработан для описания моделей данных и операций протокола NETCONF.
- **Цели:**
 - Определение конфигурационных данных для NETCONF
 - Изначально фокусируется на конфигурационной информации, но не ограничена ею
 - Может использоваться отдельно от NETCONF (не цель спецификации, но важный аспект)

Стандарты YANG



- Способ описать, что умеет сетевое устройство и в каком формате ему надо посылать запросы
- RFC7950, RFC6020
 - <https://tools.ietf.org/html/rfc6020>
 - <https://tools.ietf.org/html/rfc7950>
- Синтаксис и семантика языка YANG
- Отображение YANG на протокол управления конфигурацией сети NETCONF
- YANG использует XML для кодирования данных

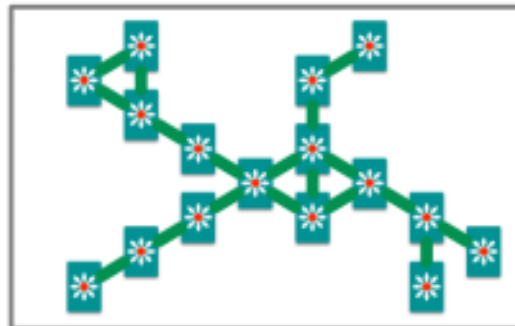


YANG Data Models



Device Data Models

- Interface
- VLAN
- Device ACL
- Tunnel
- OSPF
- etc



Service Data Models

- L3 MPLS VPN
- MP-BGP
- VRF
- Network ACL
- System Management
- Network Faults
- etc

YANG vs SNMP

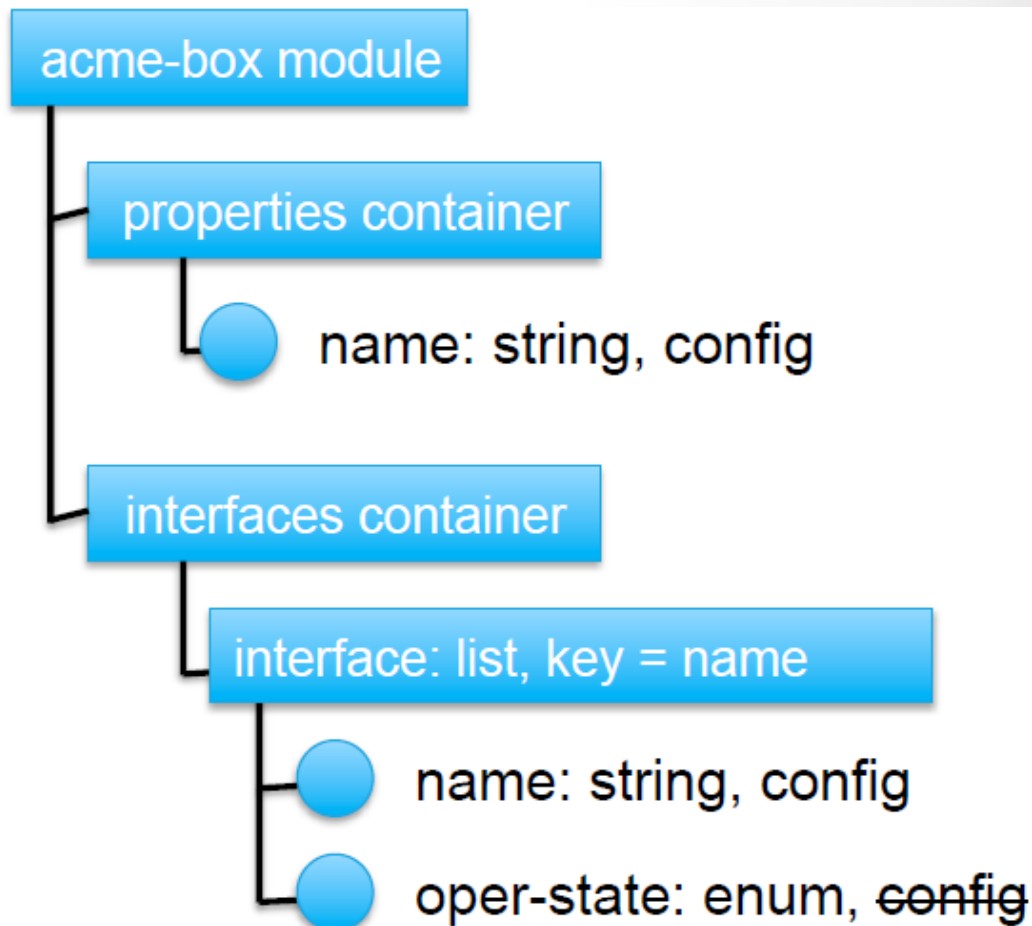


YANG в контексте NETCONF





- Язык моделирования данных
 - Данные о конфигурации
 - Данные о состоянии
- Древоподобная структура
- Данные и типы



Модель YANG заголовков



```
module acme-module {  
  namespace "http://acme.example.com/module";  
  prefix acme;  
  
  import "ietf-yang-types" {  
    prefix yang;  
  }  
  include "acme-system";  
  
  organization "ACME Inc.";  
  contact joe@acme.example.com;  
  description "Module describing the ACME products";  
  revision 2007-06-09 {  
    description "Initial revision.";  
  }  
}
```

Базовые типы YANG



- Большинство элементов YANG имеют определенный тип данных
- Тип данных может быть базовым или наследованным
 - Существует более 20 базовых типов

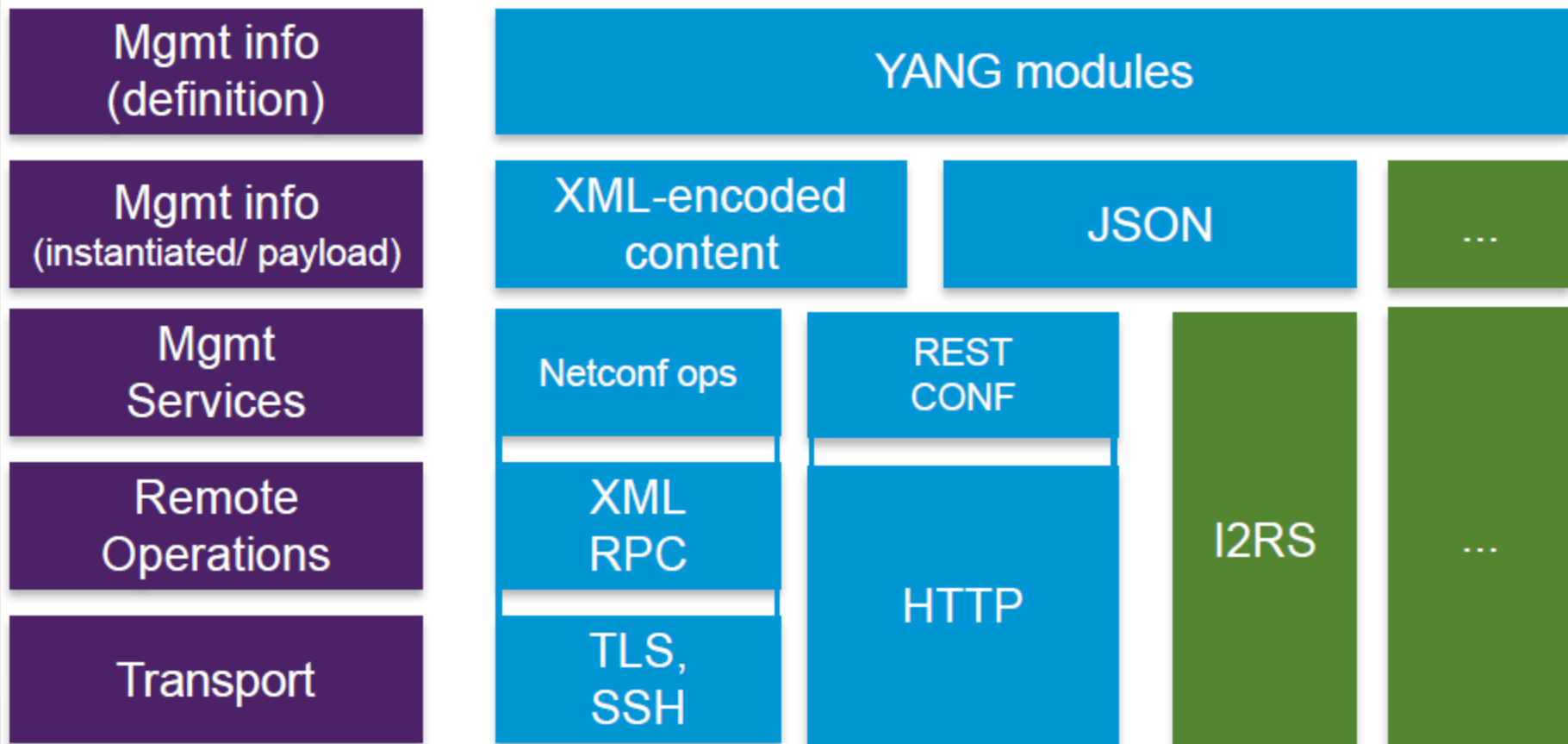
Тип данных	Значение
<code>int8/16/32/64</code>	Integer
<code>uint8/16/32/64</code>	Unsigned integer
<code>decimal64</code>	Non-integer
<code>string</code>	Unicode string
<code>enumeration</code>	Set of alternatives
<code>boolean</code>	True or false
<code>bits</code>	Boolean array
<code>binary</code>	Binary BLOB
<code>leafref</code>	Reference "pointer"
<code>identityref</code>	Unique identity
<code>empty</code>	No value, void

Операторы YANG



- Import/Include
- Typedef
- Union
- Grouping
- Choice
- List
- Leaf-list
- Key
- Unique
- RPC
- Notification
- Identity
- Must
- Augments
- Extension
- Feature
- Deviation

YANG поверх NETCONF



Достоинства модели NetConf/YANG



- Требуется только программная перепрошивка оборудования
- Все-таки хоть какая-то унификация



Спасибо за внимание!

Василий Пашков
pashkov@lvk.cs.msu.su
