제 37회 네트워크 전문가 따라잡기 N.EX.T

ICMP부터 Telemetry까지

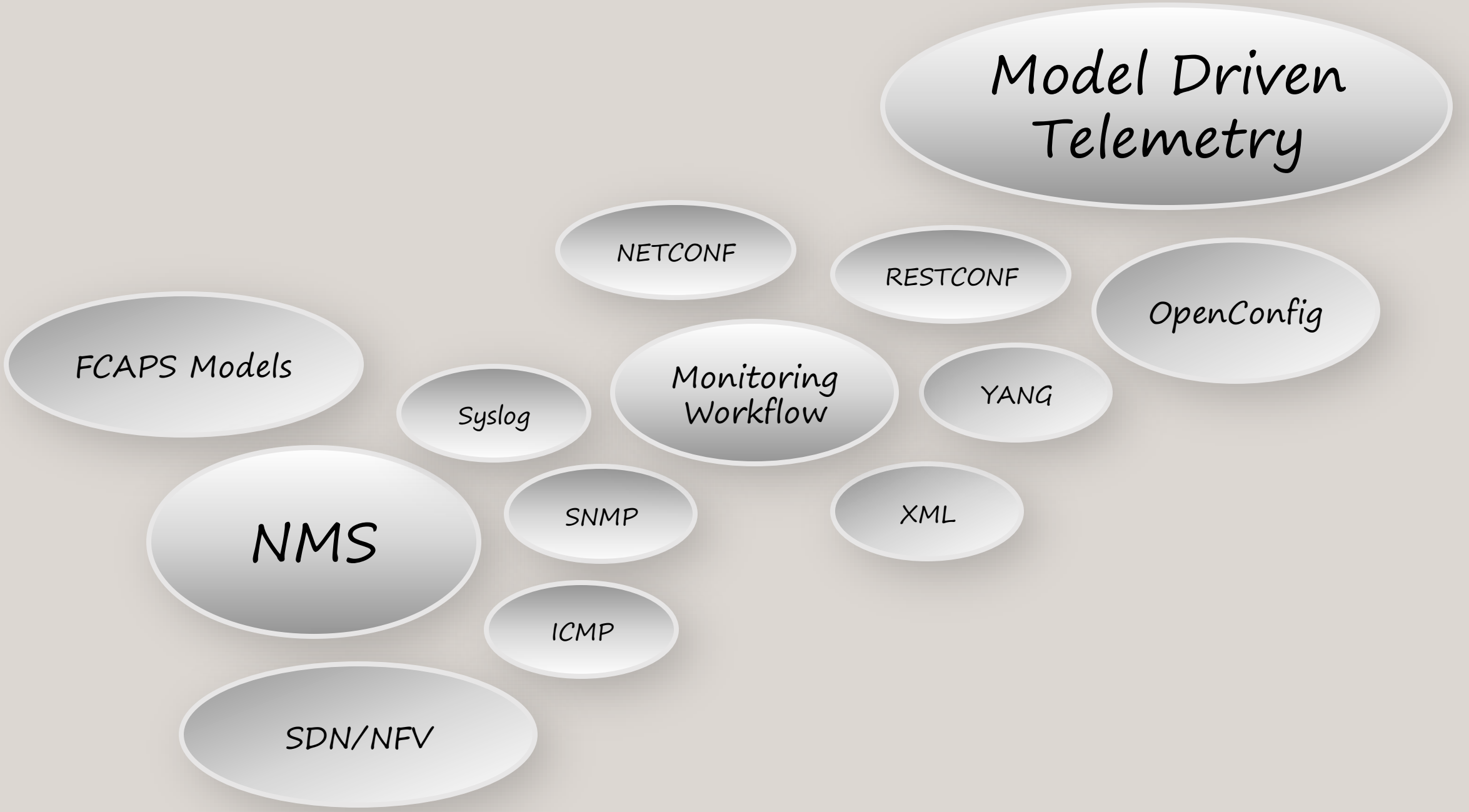
네트워크 관리 프로토콜의 진화사례 연구

2024년 11월 16일

GOODUS

저는 GOODUS 박성원 입니다.

네트워크플랫폼 을 개발하고 있습니다.


Model Driven Telemetry
NETCONF
RESTCONF
OpenConfig
FCAPS Models
Syslog
Monitoring Workflow
YANG
NMS
SNMP
XML
ICMP
SDN/NFV

NMS

ICMP부터 Telemetry까지

GOODUS

NMS, Network Monitoring / Management System

네트워크 관제 시스템 (NMS, Network Monitoring System / Network Management System) 은
컴퓨터 네트워크 또는 여러 네트워크를 모니터링하고 관리하는 데 사용되는
하드웨어와 소프트웨어의 조합을 의미합니다.

➔ NMS : 네트워크 관리자들이 네트워크의 성능, 가용성 및 보안을 효과적으로 유지 관리하기위한 필수 도구

네트워크 모니터링

- 네트워크 장비의 상태를 실시간으로 모니터링합니다.
  예: 라우터, 스위치, 서버
- 네트워크 트래픽, 대역폭 사용량 및 에러율을 추적합니다.
- 네트워크 성능 저하 또는 장애를 감지하고 경고합니다.

네트워크 관리

- 네트워크 구성을 설정하고 변경합니다.
- 네트워크 장비를 백업하고 복원합니다.
- 네트워크 보안 정책을 적용하고 시행합니다.

문제 해결

- 네트워크 문제의 근본 원인을 식별합니다.
- 네트워크 문제를 해결하고 성능을 최적화합니다.
- 네트워크 문제 발생 시 보고서를 생성합니다.

The Concept of Network Management

네트워크 관리 (Network Management) 는
여러 네트워크 장치를 관리하는 관리자를 돕기 위한 다양한 시스템, 기술, 도구를 사용하는 일반적인 네트워크 관리 개념으로
1997년 8월 ISO 표준화 기구에서 FCAPS 모델로 명명되어 OSI 관리 프레임워크로 제정되었습니다.

➔ OSI Management Framework - CCITT Rec. X.700 | ISO/IEC 7498-4) | 1997-08-09

Fault Management

- 시스템 또는 네트워크에서 발생한 물리적 장애 감지 및 알림

Configuration Management

- 시스템 또는 네트워크에서 사용하는 여러 버전의 소프트웨어/하드웨어 요소들의 추적, 관리
- 네트워크와 시스템 구성 모니터링

Accounting Management

- 시스템 또는 네트워크 자원에 접근하는 모든 개인 및 집단의 올바른 권한 및 책임 관리

Performance Management

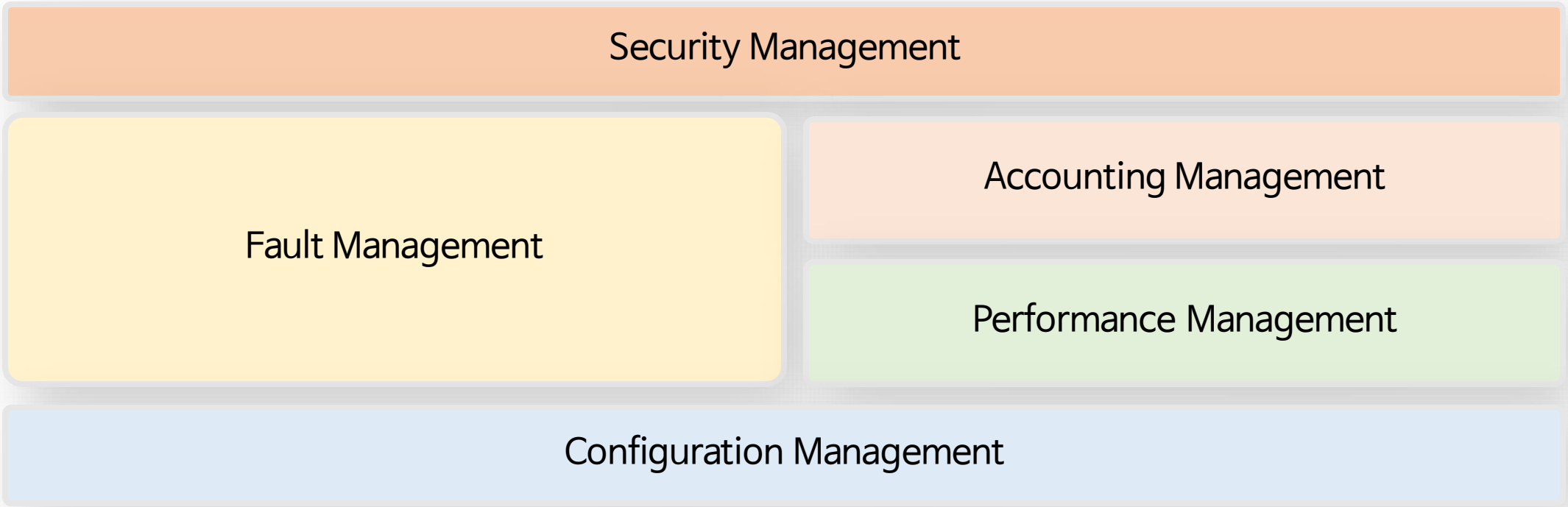
- 시스템 또는 네트워크의 다양한 성능 지표 측정 및 보고

Security Management

- 시스템 또는 네트워크 자원에 대한 접근 제어
- 시스템이나 네트워크를 위협하는 공격 감지 및 보호

FCAPS Model Levels

FCAPS 는 네트워크 관리의 주요 관점을 범주화한 모델의 약어이며, 네트워크 및 시스템 관리자가 다양한 문제를 이해하고 극복할 수 있는 지식을 제공하는 데 도움이 됩니다.



TMN and FCAPS Management Model

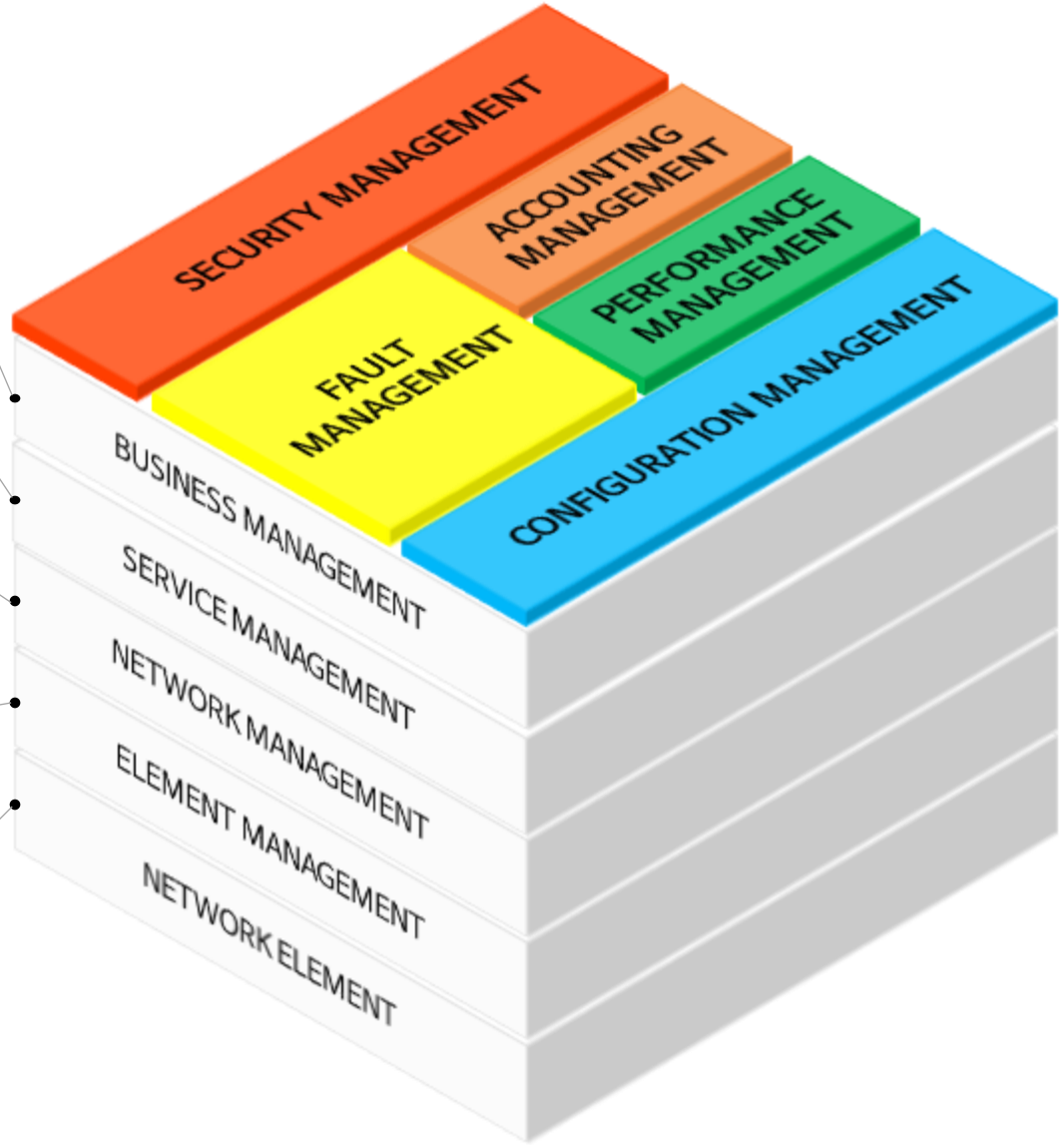
- Billing
- Financial Reports
- Business Trends

- Service Definition
- Service Monitoring
- Service Charging

- Network Configuration
- Resource Control
- QoS Provisioning

- Alarm Management
- Logging & Backup
- H/W, S/W Maintenance

- Agent Services
- Mapping physical aspects of device to TMN



- Identify & Isolate Faults
- Log & Correct Faults
- Predict Faults

- Configuration of NE
- Plan network expansion

- Billing Management
- Usage Statistics

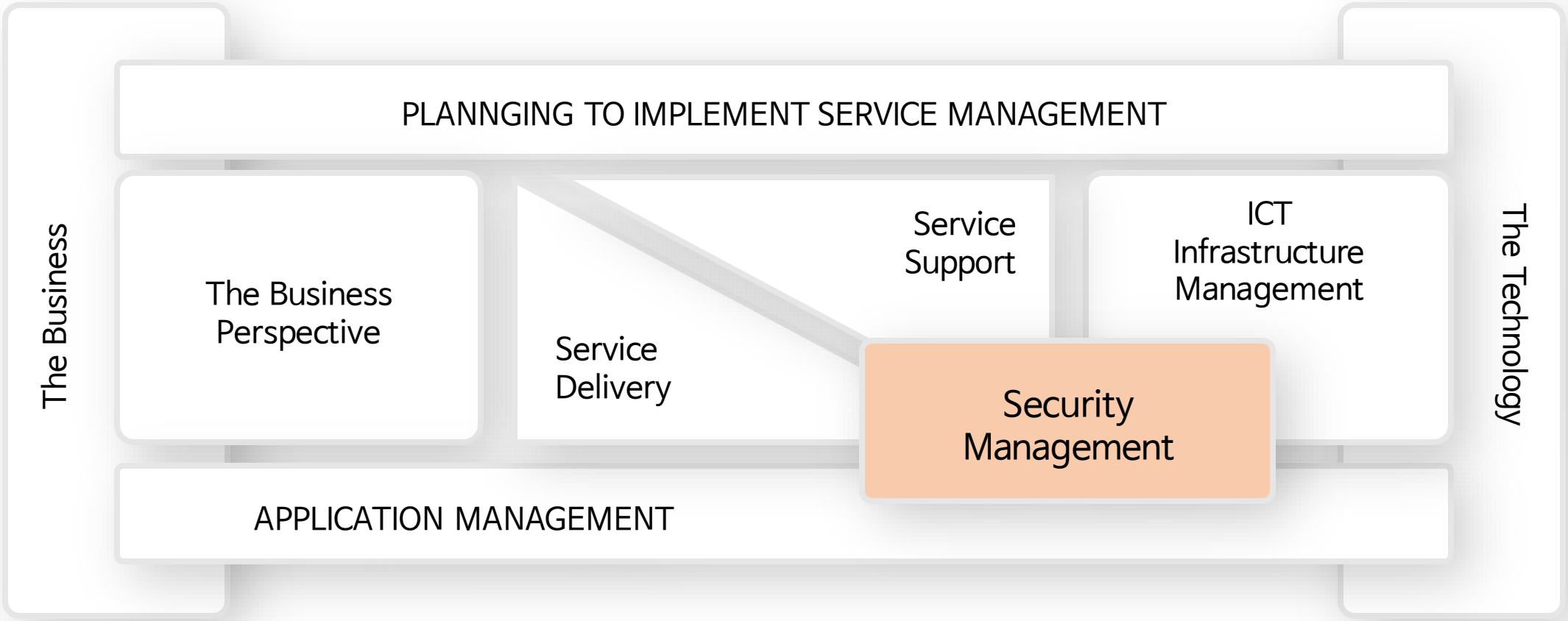
- Utilization Monitoring
- QoS Management
- Resource Provisioning

- Authorization
- Authentication
- Encryption

TMN, Telecommunication Management Network

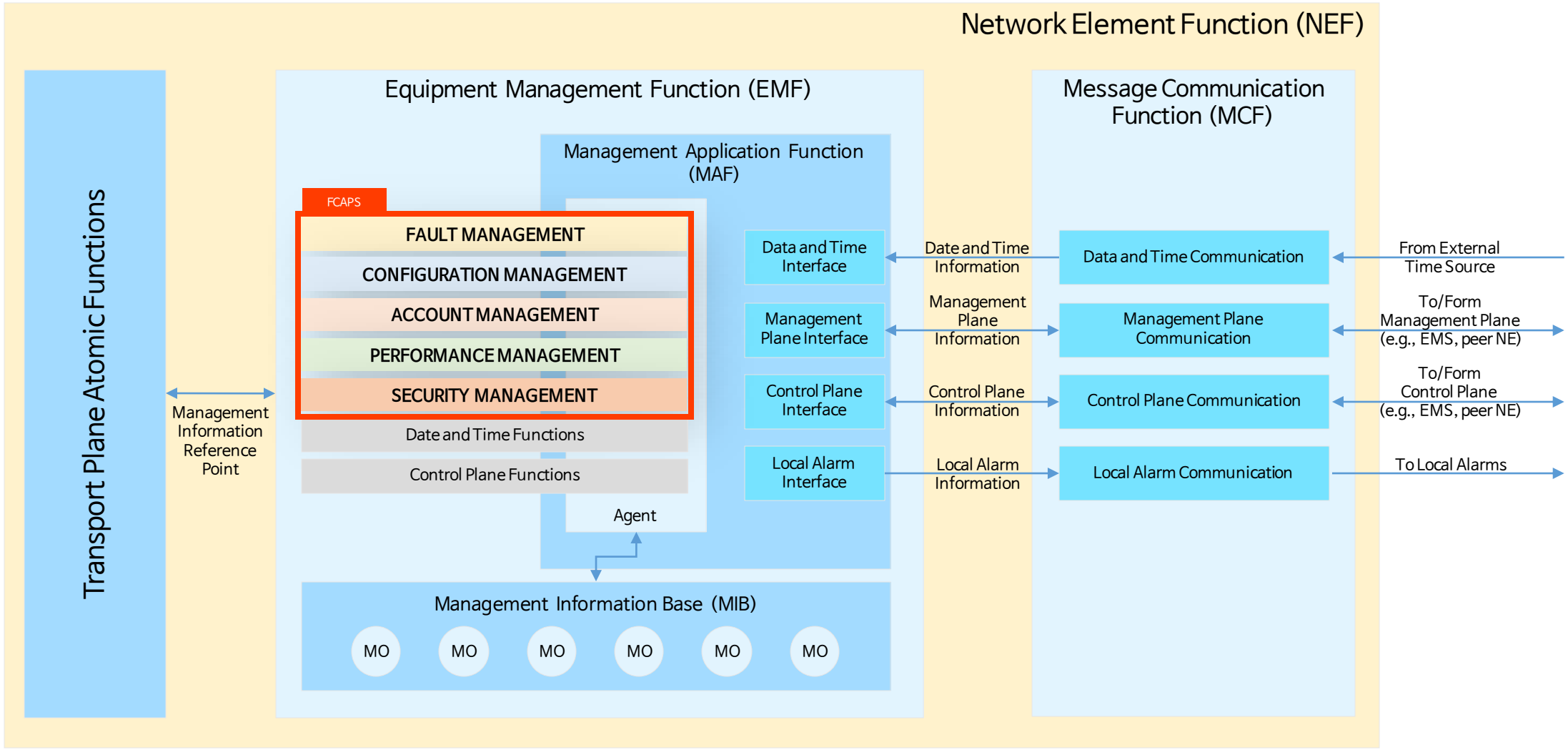
ITIL & FCAPS - Network Management Fundamentals

ISO/IEC 20000 표준인 ITIL은 IT 서비스를 비즈니스 요구사항에 맞게 조정하는 데 중점을 둔 IT 서비스 관리를 위한 일련의 관행입니다. ITIL은 조직에서 최소한의 역량을 구축하기 위해 사용하는 절차, 작업 및 체크리스트를 설명합니다.



ITIL, Information Technology Infrastructure Library

NEF/EMF/MAF/MCF의 FCAPS 컨셉



NEF, Network Element Function / EMF, Equipment Management Function / MAF, Management Application Function / MCF, Message Communication Function / MO, Managed Object

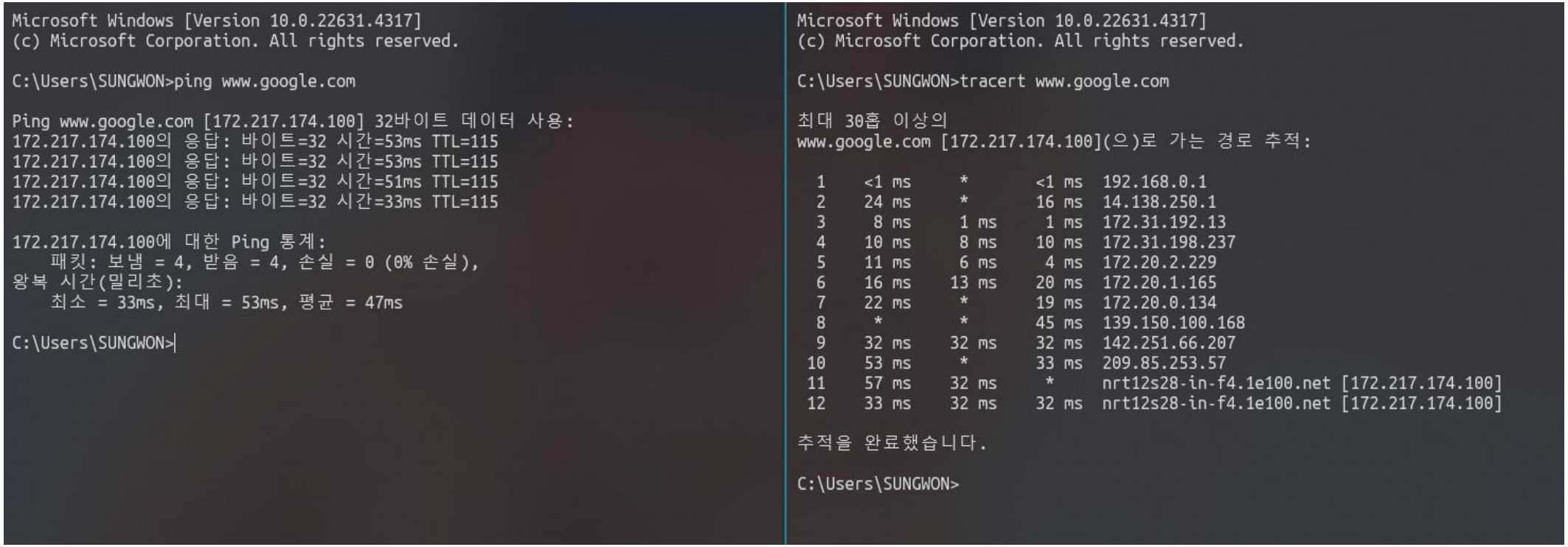
ICMP, SNMP, Syslog

ICMP부터 Telemetry까지

GOODUS

ICMP

- ICMP (Internet Control Message Protocol) 는 네트워크 장치에서 네트워크 통신 문제를 진단하는 데 사용하는 네트워크 계층 프로토콜, 주로 데이터가 의도한 대상에 적시에 도달하는지 여부를 확인하는데 사용됨 (ping, tracert/traceroute)

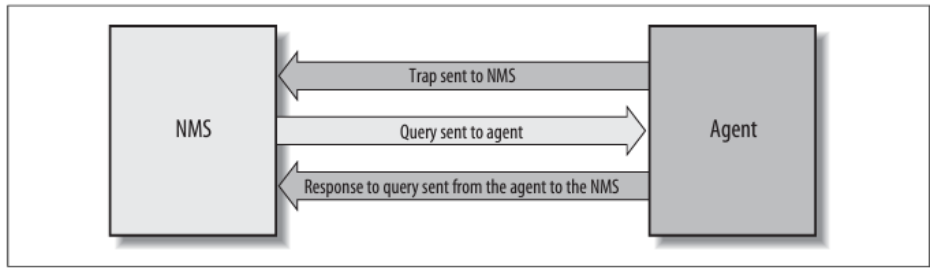


```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SUNGWON>ping www.google.com

Ping www.google.com [172.217.174.100] 32바이트 데이터 사용:
172.217.174.100의 응답: 바이트=32 시간=53ms TTL=115
172.217.174.100의 응답: 바이트=32 시간=53ms TTL=115
172.217.174.100의 응답: 바이트=32 시간=51ms TTL=115
172.217.174.100의 응답: 바이트=32 시간=33ms TTL=115

172.217.174.100에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 33ms, 최대 = 53ms, 평균 = 47ms

C:\Users\SUNGWON>
```

```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SUNGWON>tracert www.google.com

최대 30홉 이상의
www.google.com [172.217.174.100](으)로 가는 경로 추적:

  1    <1 ms     *       <1 ms  192.168.0.1
  2    24 ms     *       16 ms  14.138.250.1
  3     8 ms     1 ms     1 ms  172.31.192.13
  4    10 ms     8 ms    10 ms  172.31.198.237
  5    11 ms     6 ms     4 ms  172.20.2.229
  6    16 ms    13 ms    20 ms  172.20.1.165
  7    22 ms     *       19 ms  172.20.0.134
  8     *        *       45 ms  139.150.100.168
  9    32 ms    32 ms    32 ms  142.251.66.207
 10    53 ms     *       33 ms  209.85.253.57
 11    57 ms    32 ms     *     nrt12s28-in-f4.1e100.net [172.217.174.100]
 12    33 ms    32 ms    32 ms  nrt12s28-in-f4.1e100.net [172.217.174.100]

추적을 완료했습니다.

C:\Users\SUNGWON>
```

SNMP

- SNMP (Simple Network Management Protocol) 는 시스템 또는 네트워크를 원격으로 모니터링하고 관리하는 데 사용되는 표준 프로토콜
  - SNMP 매니저(매니지먼트S/W, NMS): SNMP 에이전트를 모니터링하고 관리하는 소프트웨어 (서버)
  - SNMP 에이전트(Agent): 네트워크장비에서 관리정보 수집 및 SNMP관리자 요청 응답 (클라이언트)
  - SNMP 관리정보기준(MIB): SNMP 에이전트가 관리하는 정보를 정의 (서버의 요청에 응답하기 위한 데이터 참조 값)



- snmpwalk, snmpget 명령어와 OID 를 사용하여 시스템 또는 네트워크의 정보를 수집할 수 있습니다.

$ snmpwalk -v 2c -c public 10.20.5.22

```
sungwon@SUNGWON-ONYX:~$ snmpwalk -v 2c -c public 10.20.5.22
iso.3.6.1.2.1.1.1.0 = ""
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.674.10892.5
iso.3.6.1.2.1.1.3.0 = Timeticks: (700181323) 81 days, 0:56:53.23
iso.3.6.1.2.1.1.4.0 = STRING: "\"support@dell.com\""
iso.3.6.1.2.1.1.5.0 = STRING: "iDRAC-J634DJ3"
iso.3.6.1.2.1.1.6.0 = STRING: "\"unknown\""
iso.3.6.1.2.1.1.8.0 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for managing IP and ICMP implementations"
```

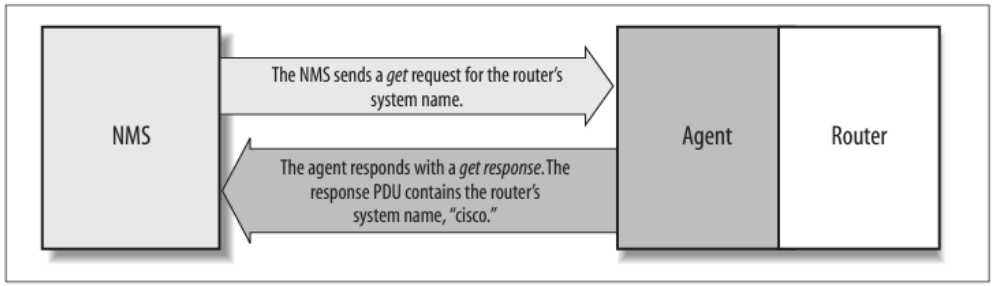
$ snmpget -v 2c -c public 10.20.5.22 iso.3.6.1.2.1.1.5.0

```
sungwon@SUNGWON-ONYX:~$ snmpget -v 2c -c public 10.20.5.22 iso.3.6.1.2.1.1.5.0
iso.3.6.1.2.1.1.5.0 = STRING: "iDRAC-J634DJ3"
sungwon@SUNGWON-ONYX:~$
```

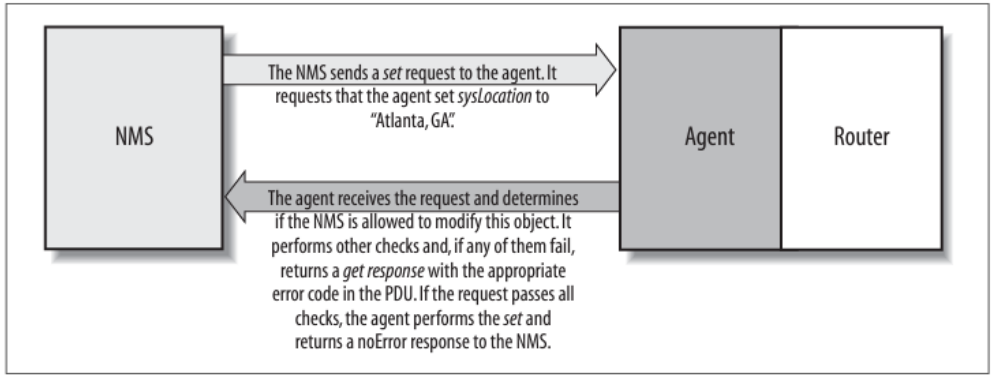
SNMP

- snmpget, snmpset, getnext, getbulk, getresponse, trap, notification, inform, report 등 다양한 SNMP 명령어들

```
$ snmpget -v 1 -c public cisco.ora.com .1.3.6.1.2.1.1.6.0

$ snmpget -v 1 -c public 127.0.0.1 sysContact.0

$ snmpget -v 2c -c public 127.0.0.1 sysContact.0
```

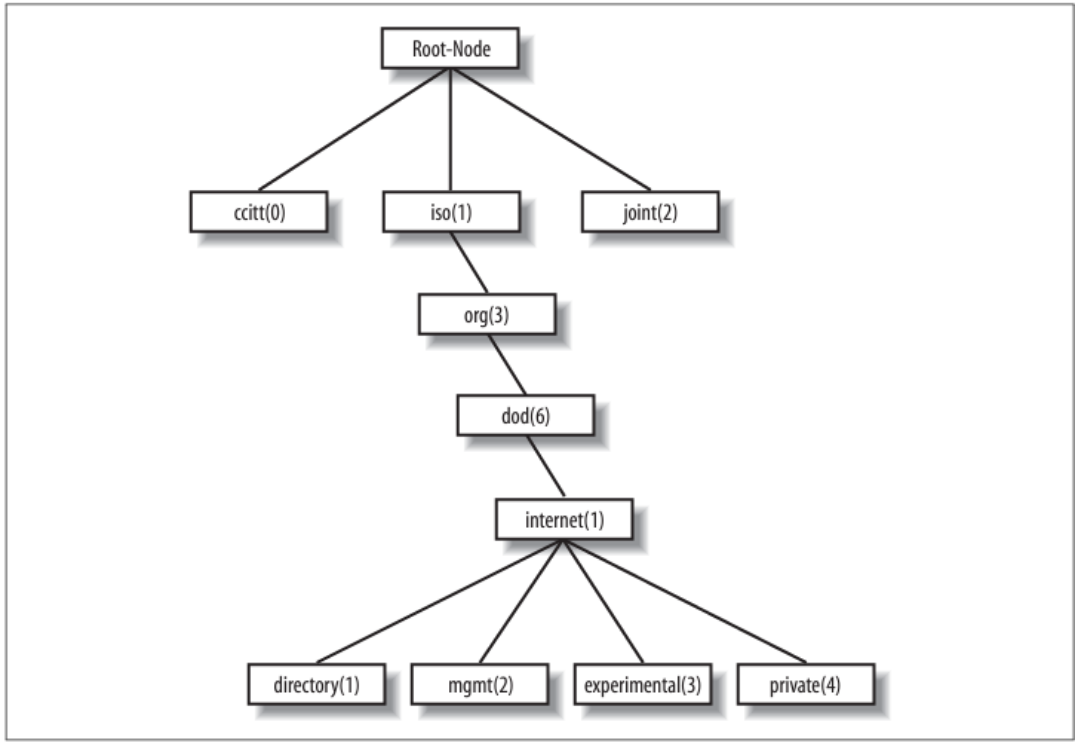


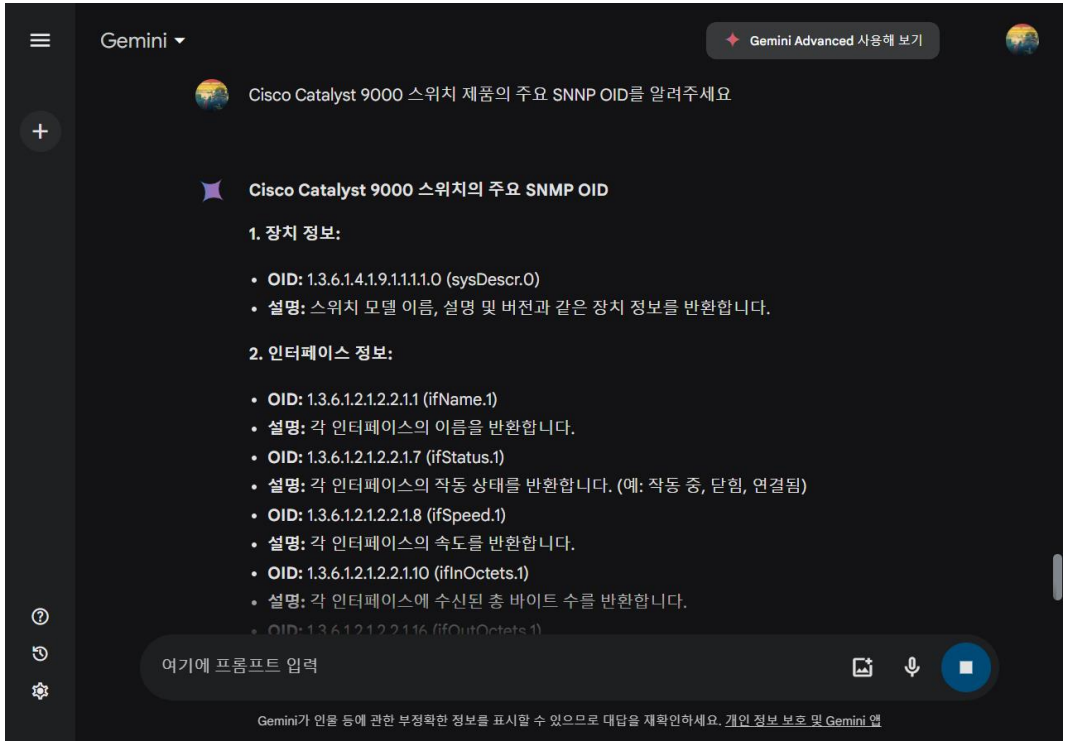

```
% snmpget -v 2c -c demopublic test.net-snmp.org ucdDemoPublicString.0
enterprises.ucdavis.ucdDemoMIB.ucdDemoMIBObjects.ucdDemoPublic.ucdDemoPublicString.0 = "hi there“

% snmpset -v 2c -c demopublic test.net-snmp.org ucdDemoPublicString.0 s "hello world"
enterprises.ucdavis.ucdDemoMIB.ucdDemoMIBObjects.ucdDemoPublic.ucdDemoPublicString.0 = "hello world“

% snmpget -v 2c -c demopublic test.net-snmp.org ucdDemoPublicString.0
enterprises.ucdavis.ucdDemoMIB.ucdDemoMIBObjects.ucdDemoPublic.ucdDemoPublicString.0 = "hello world"
```



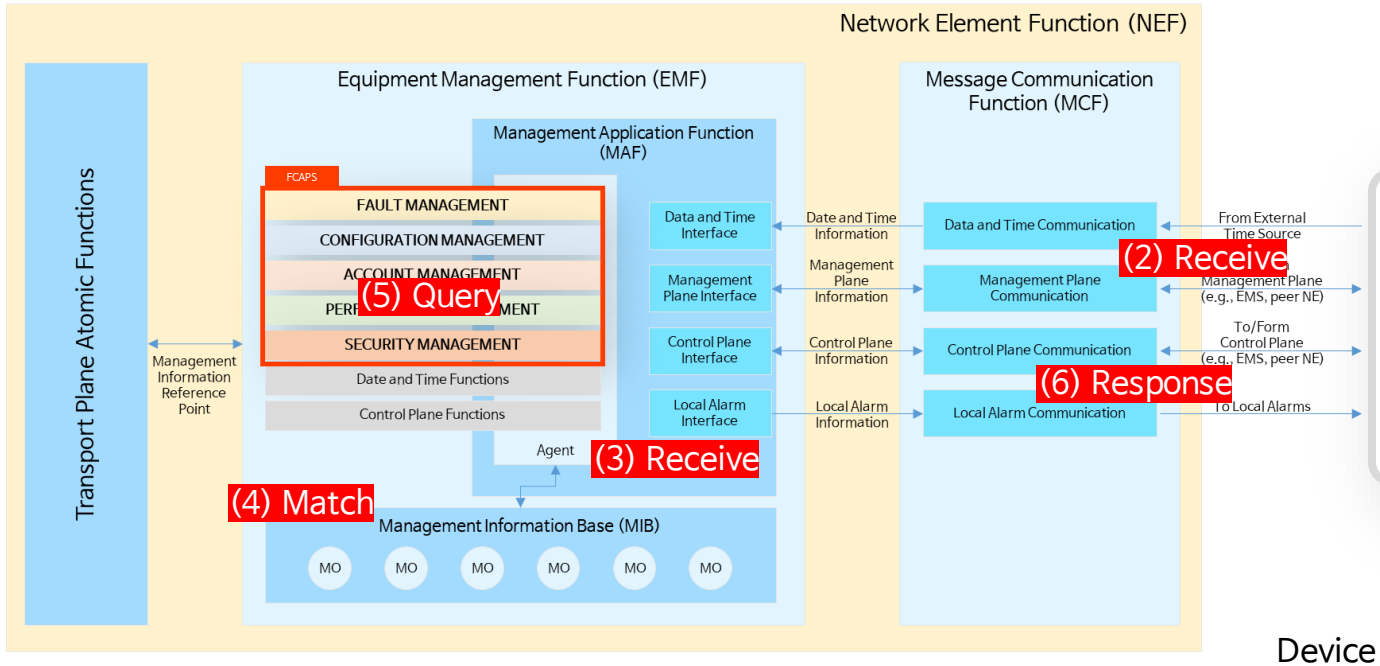
SNMP, OID

- OID : Object IDentifier (객체식별자)
- MIB : Management Information Base (관리정보데이터베이스 객체식별자)





SNMP, NMS



SNMP 매니저 (매니지먼트S/W, NMS)

Device Information | Auto Discovery (LLDP/CDP) | Asset Management

Network Operation Center | AI / Chatbot | Collect Item | MIB/OID Store | Query Configuration (Version, Community)

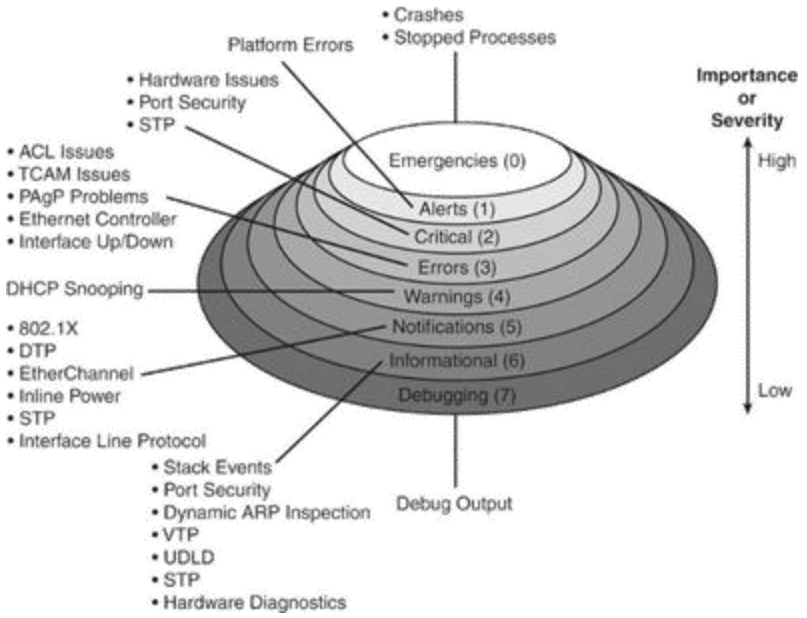
Predictive Analysis / Anomaly Detection | Job Schedule | Data Preparation, Post-Processing | Data Store

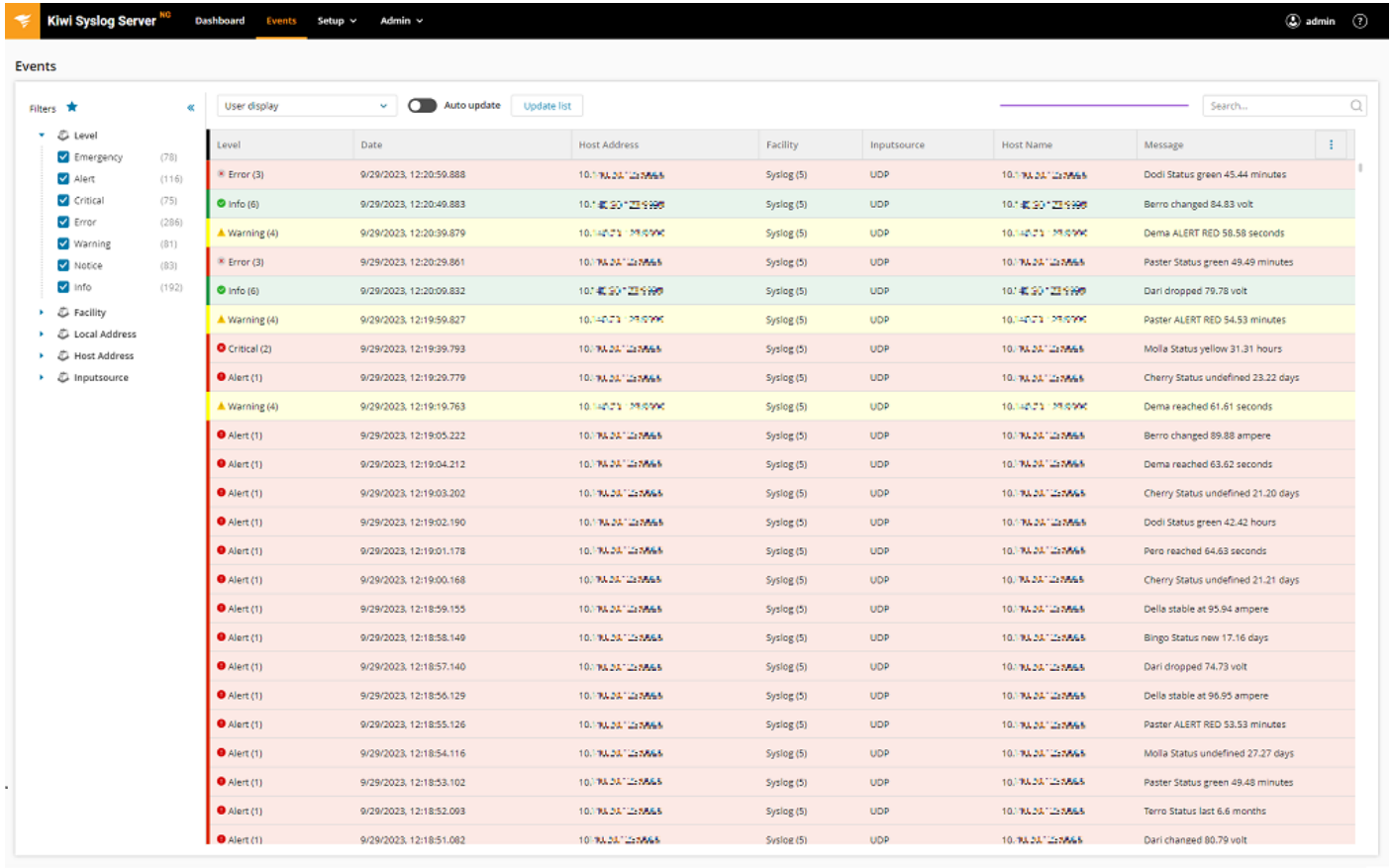
Provisioning | Change Management | Report | Event (Thresholds, Keyword) | Alarm | Notification

Maintenance Automation | Config Backup, Compare, Restore | Access Control | Issue | Account Management

Syslog

- Syslog 는 메시지 로깅을 위한 표준으로 메시지를 생성하는 소프트웨어, 이를 저장하는 시스템, 이를 보고 및 분석하는 소프트웨어를 분리





ICMP, SNMP, Syslog

	ICMP	SNMP	Syslog
목적	네트워크 연결 진단 및 오류 보고	네트워크 장비의 관리 및 모니터링	시스템 및 네트워크 이벤트 로깅
주요기능	도달성 테스트 (PING), 경로 추적 (traceroute), 네트워크 오류 및 상태 메시지 전송	상태 정보 및 성능 데이터 수집, 장비 설정 변경, 이벤트 알림(Trap) 전송	로그 메시지 수집 및 전송, 중앙 집중식 로그 관리
활용방안	네트워크 상태 점검, 라우팅 문제 진단	네트워크 성능 모니터링, 구성 관리 및 장애 대응	보안 모니터링, 시스템 및 네트워크 이벤트 분석
특징	IP 네트워킹의 핵심 프로토콜, 간단한 진단 도구로 활용	버전별 보안 기능 강화 (v1/v2, v3), 폴링 및 트랩 매커니즘으로 실시간 모니터링 및 알림 기능 제공	다양한 장비와 시스템과의 호환성, 보안 감사 및 규정 준수

NMS Workflow

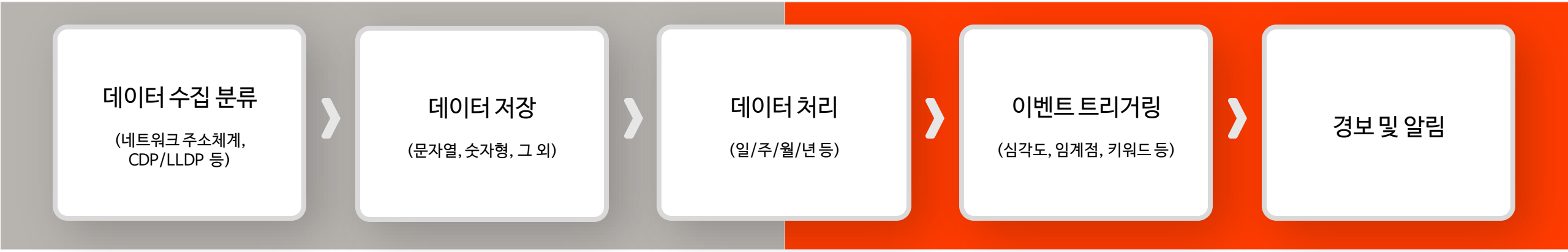
- 모니터링 대상 및 수집항목, 수집데이터 보관 주기를 결정합니다.

Network Element 수량 확인	Network Interface 확인	Collect Item 확인	성능 수집 주기	데이터 보관 주기
(Network, System …)	(Physical, Logical, Virtual …)	(CPU/MEM, Temperature) 그 외 I/F 별 수집항목 설정 회선사용량(in/out), 회선사용률(in/out), 패킷처리량(in/out), 회선 error(in/out), multicast(in/out), broadcast(in/out), ifdiscard(in/out)	(기본 60초)	(SNMP, Syslog 데이터)

- NE 10K 규모를 모니터링 한다고 가정해보겠습니다.
  - 1회 수집 시 인스턴스 : (3 + (24 * 50%) * 14) * 10,000 = 1,710,000 인스턴스
  - 1일 수집 시 인스턴스 : 1,710,000 * 60 * 24 = 2,462,400,000 인스턴스 (24.6억개 인스턴스 수집)
  - 1일 디스크 사용량은 약 19.7GB 입니다. (인스턴스 당 8 Byte만 사용한다고 가정하는 경우)
  - 1초당 28,500 건의 데이터 처리 필요가 필요합니다.

초당 약 28,500 건의 데이터 처리를 위한 노력들

- 초당 약 28,500 건의 데이터 처리를 위해서는 다양한 선처리 및 후처리 과정이 필요합니다.



- 데이터 수집 분류, 데이터 저장, 데이터 처리, 이벤트 트리거링, 데이터 분석 등 일련의 과정을 통해 NMS 시스템은 동작합니다.
- 초당 약 2.8만회의 데이터 처리는 분산처리, 병렬처리 등 고급 프로그래밍 기술이 필요하며, 다양한 데이터 스토리징 기술, 메시지 브로커리 기술 등 스트림 데이터 처리를 위한 연계와 콤플렉스 이벤트 프로세싱 기법 등이 필요합니다.
- 이벤트 트리거링은 저장, 처리 된 데이터를 기반으로 NMS 를 사용하는 네트워크 관리자에게 적절한 경보와 알림서비스를 제공하며, 외부 시스템과의 연계(이메일, SMS/LMS, IM 등)를 수행할 수 있어야 합니다.

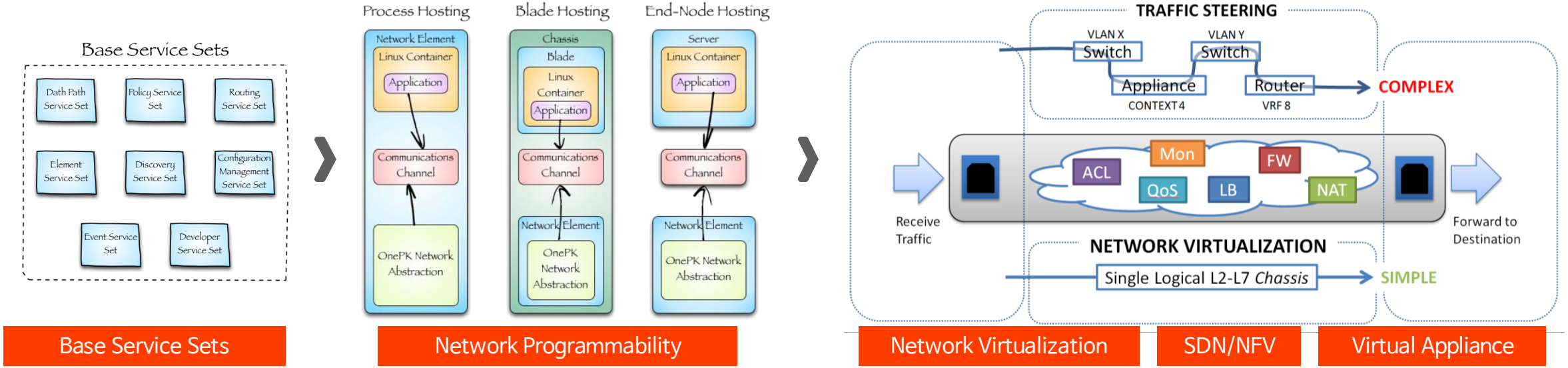
Virtualization, SDN/NFV

ICMP부터 Telemetry까지

GOODUS

Network Virtualization, SDN/NFV

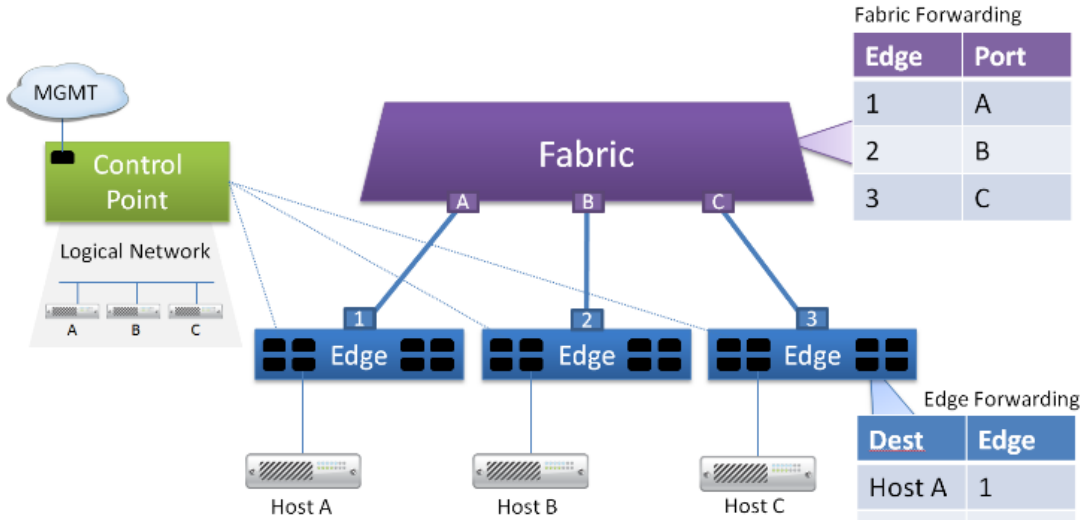
- 네트워크 가상화를 기반으로 한 네트워크 기본 서비스 셋의 배포는 다양한 배포 모델을 기반으로 네트워크 플로우를 제어하는 포워딩 파이프라인을 형성합니다. 네트워크 프로그래밍은 소프트웨어를 사용하여 네트워크 요소를 배포, 관리 및 문제 해결하는 것을 말합니다. 프로그래밍 가능한 네트워크는 비즈니스 요청이나 네트워크 이벤트에 따라 조치를 취할 수 있는 지능형 소프트웨어 스택에 의해 구동됩니다.



Base Service Sets | Network Programmability | Network Virtualization | SDN/NFV | Virtual Appliance

- 네트워크 프로그래밍 기능을 보완하는 소프트웨어 정의 네트워킹(SDN)은 네트워크 요소의 컨트롤플레인과 데이터플레인을 분리할 뿐만 아니라 이를 제어하고 관리하기 위한 API도 제공합니다.

Modular Chassis Platform vs. Network Virtualization Chassis

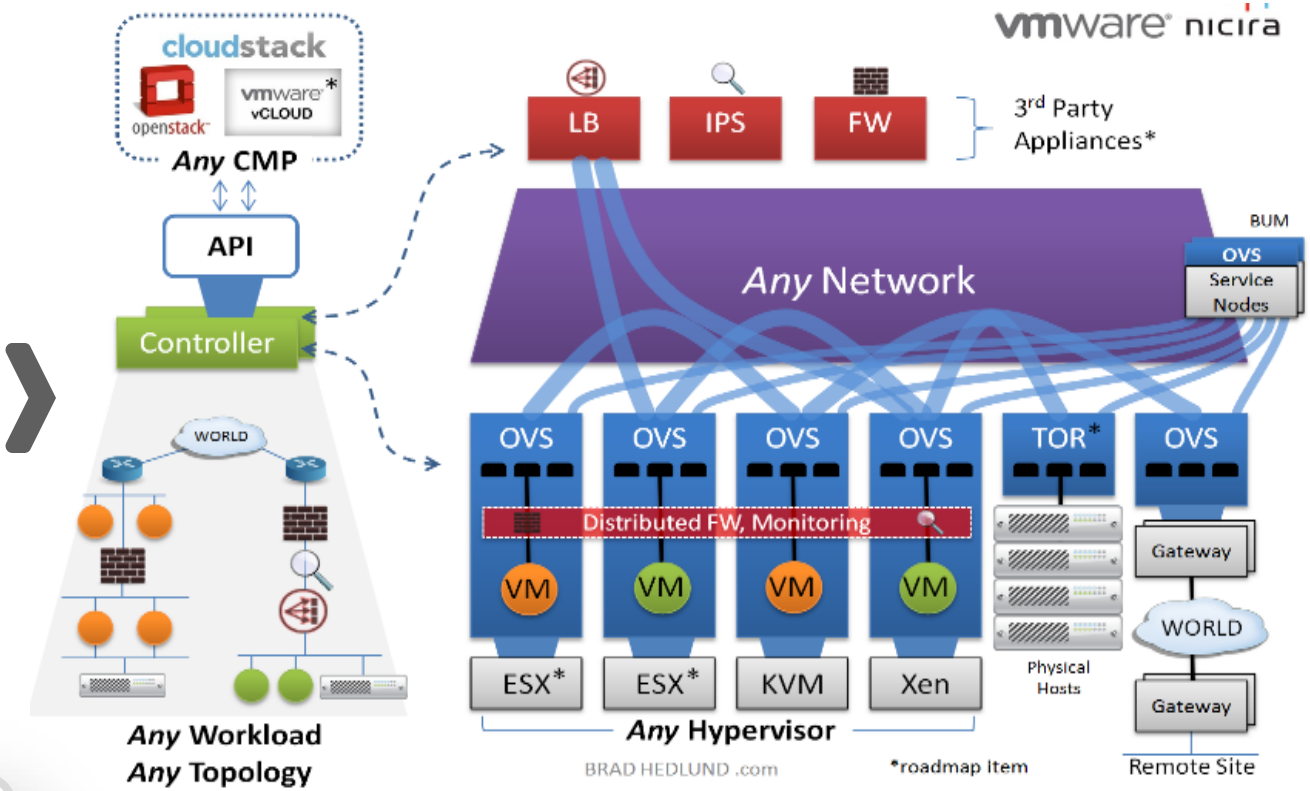


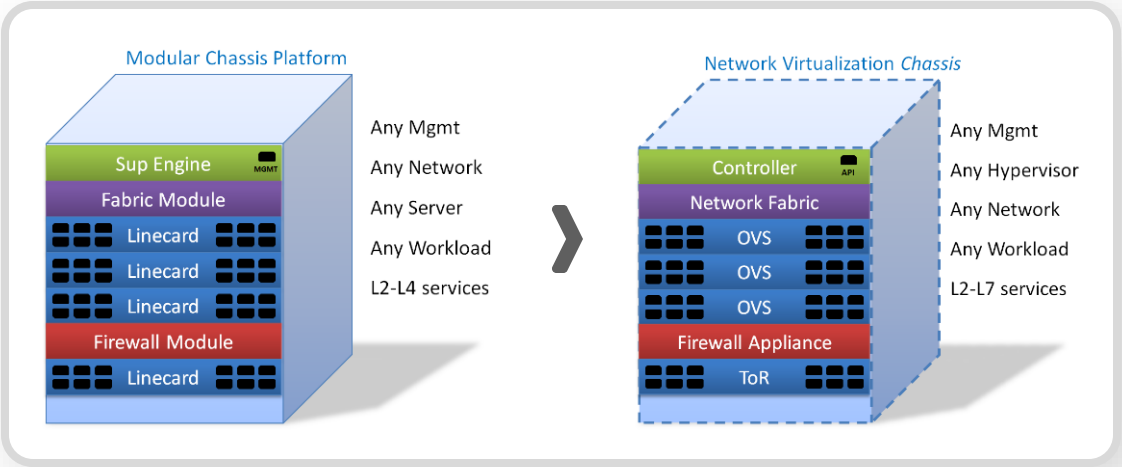
Fabric Forwarding

Edge	Port
1	A
2	B
3	C

Edge Forwarding

Dest	Edge
Host A	1
Host B	2
Host C	Local

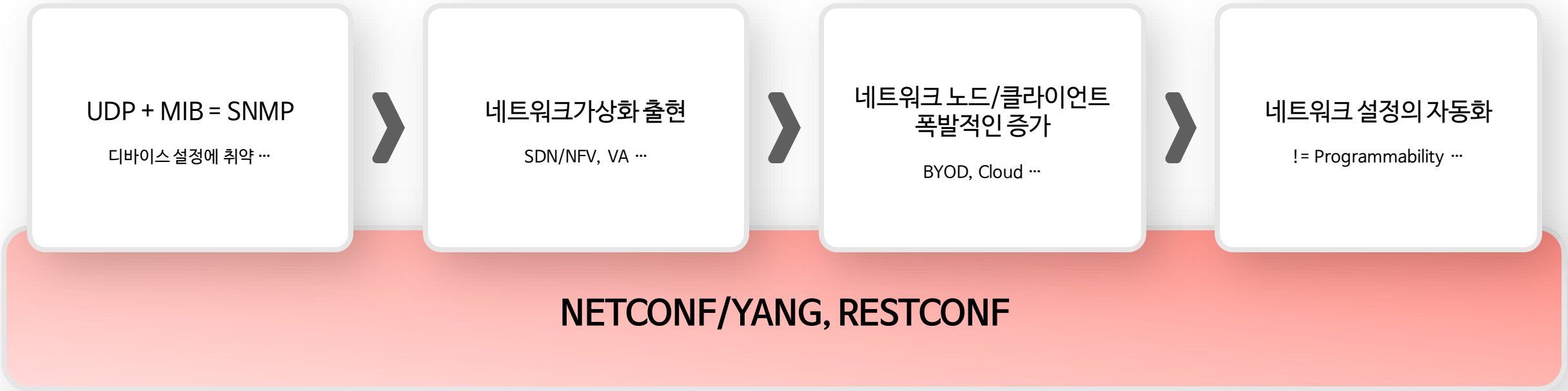




- 모듈라 타입의 샤시형 장비에서 네트워크 가상화를 제공하는 컴퓨트 시스템으로 전환되어 네트워크 프로그래밍 기술이 부상하였습니다. 네트워크 프로그래밍은 소프트웨어를 사용하여 네트워크 요소를 배포, 관리 및 문제 해결하는 것을 말합니다.

네트워크 프로그래밍의 필요성

- 네트워크 가상화 시대에서 UDP 기반의 SNMP 서비스는 너무 느리고, snmpset 명령어 만으로는 네트워크 서비스 설정에 필요한 충분한 기능이 제공되지 못했습니다.
- 네트워크 가상화로의 아키텍처 전환과 폭발적인 네트워크 노드의 증가로 네트워크 설정의 자동화와 실시간 서비스 전환은 필수 요소로 자리잡았습니다.



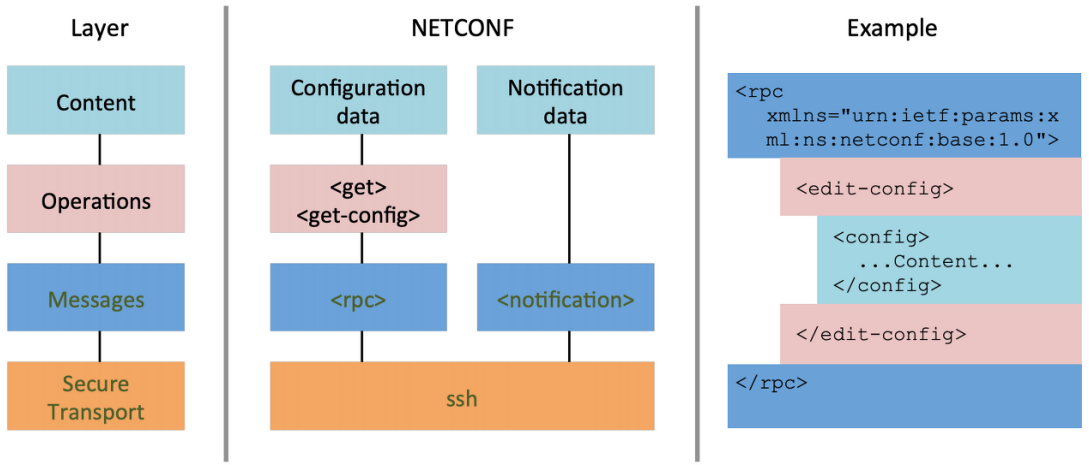
NETCONF/YANG, RESTCONF

ICMP부터 Telemetry까지

GOODUS

NETCONF/YANG

- NETCONF : 네트워크 가상화에 따른 복잡성 등 다양한 네트워크 관리 이슈를 해결하고자 IETF NETCONF 워킹그룹에서 표준화한 네트워크 관리 프로토콜(RFC 6241)로써, TCP/SSH 위에서 XML 포맷으로 네트워크 컨피그 정보를 정의하는 응용계층 프로토콜 ➔ Network Configuration
- YANG은 Yet Another Next Generation의 줄임말로 IETF NETMOD 워킹그룹 표준화한 데이터 모델링 언어(RFC 6020)이며, NETCONF로 데이터를 전달하기 위한 데이터 모델링을 위해 사용 ➔ Network Modeling




```
<!-- NETCONF XML -->
<user>
 <name>glocks</name>
 <full-name>Goldie Locks</full-name>
 <class>intruder</class>
</user>
<user>
  <name>snowey</name>
  <full-name>Snow White</full-name>
  <class>free-loader</class>
</user>
<user>
  <name>rzell</name>
  <full-name>Rapun Zell</full-name>
  <class>tower</class>
</user>
```

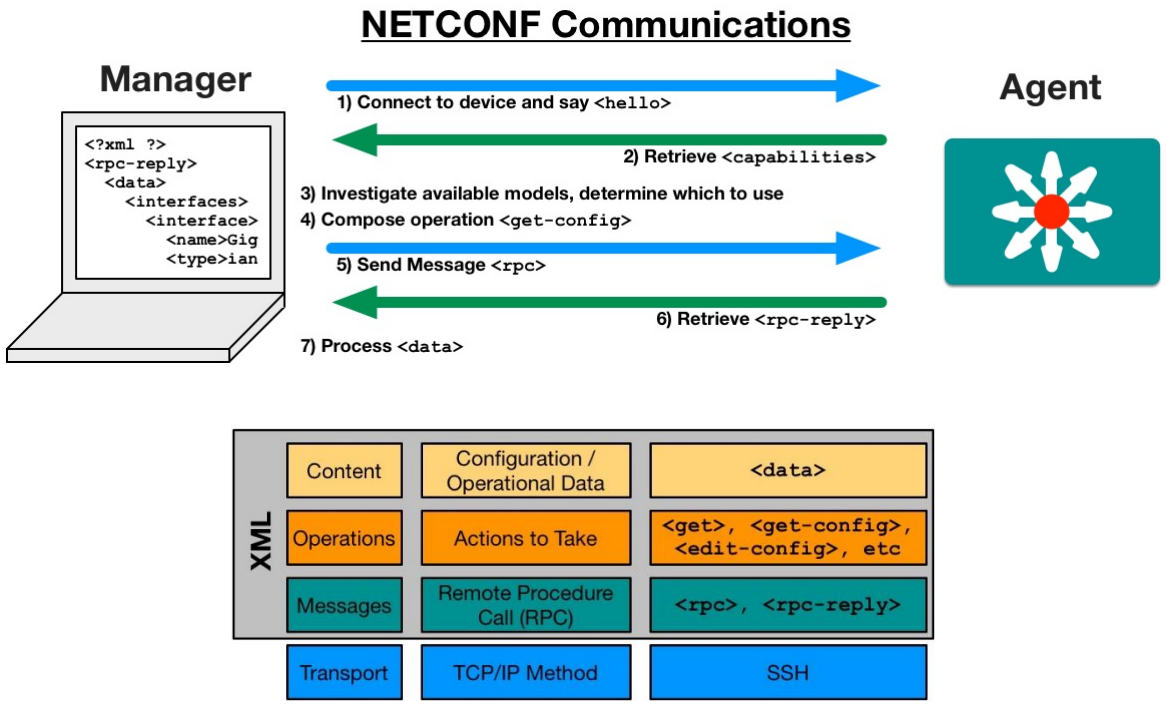
```
/* YANG model */
list user {
    key "name";
    leaf name {
        type string;
    }
    leaf full-name {
        type string;
    }
    leaf class {
        type string;
    }
}
```

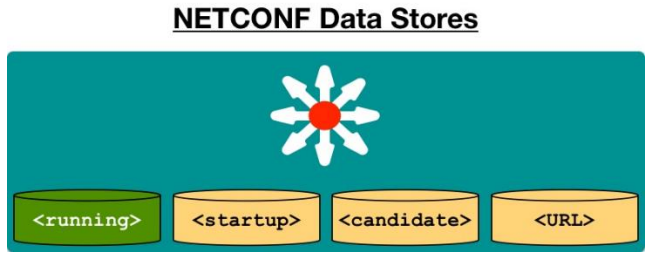
- 컨피그 매니지먼트만을 고민한 프로토콜
- 기존 CLI 방식에서 할 수 없었던 데이터 모델(XML)을 사용
- 에러 정보에 대한 관리체제 확보

- 누구나 쉽게 읽고, 쉽게 작성할 수 있는 표현 방식을 제공
- 잘 설계된 모델링 언어를 이용한 네트워크 장비와의 커뮤니케이션 확보
- SNMP로 표현할 수 없는 데이터에 대한 제약 사항을 완화, 검증 기능 제공

NETCONF Communications & Data Stores

- NETCONF/YANG 을 이용한 모델 기반 텔레매트리(원격측정) 아키텍처는 IETF가 SNMP 대체를 고려하여 주요 기준을 마련했습니다. 이러한 기준을 충족하기 위해 NETCONF에는 각 이벤트의 기능을 제공하는 “데이터 저장소”가 포함되며, 해당 데이터 저장소는 컨피그를 실행하기 전에 사전 검증할 수 있는 컨피그 데이터의 사본을 보관합니다.
  - 컨피그 유효성 검사를 위한 통합 방법론 / 오류 확인 및 조치 방안 / 롤백

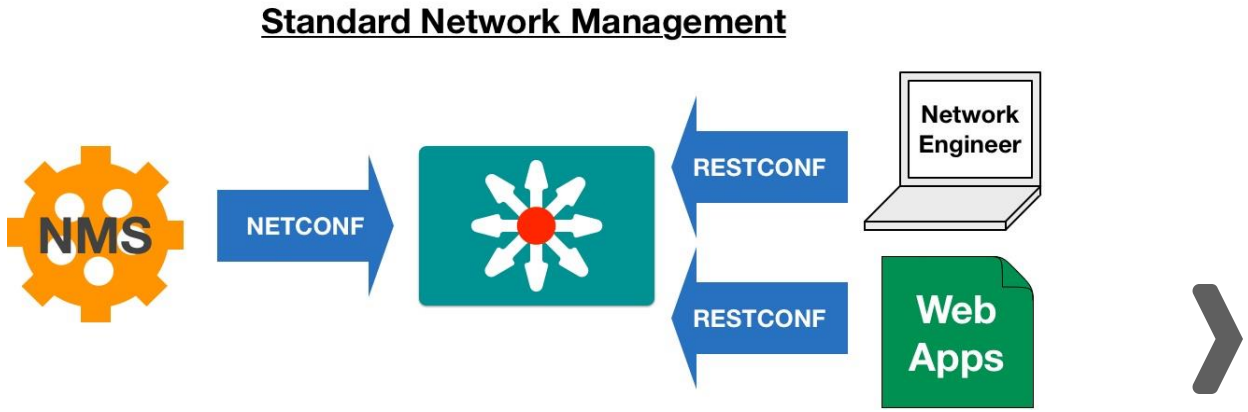


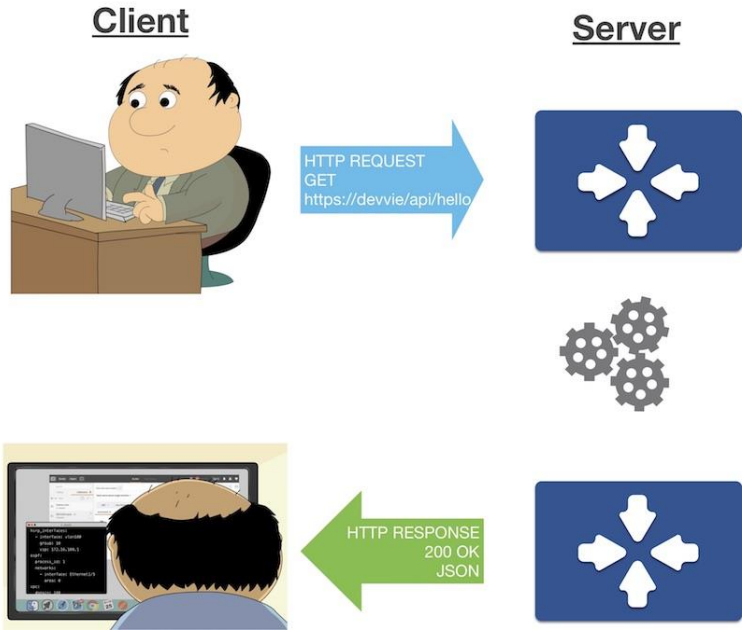


Operation	Description
<get>	Retrieve running configuration and device state information.
<get-config>	Retrieve all or part of specified configuration datastore.
<edit-config>	Load all or part of a configuration to the specified configuration datastore.
<copy-config>	Replace an entire configuration datastore with another.
<delete-config>	Delete a configuration datastore.
<commit>	Copy candidate datastore to running datastore.
<lock> / <unlock>	Lock or unlock the entire configuration datastore computer.
<close-session>	Close the NETCONF session gracefully.
<kill-session>	Force the NETCONF session to end.

RESTCONF

- NETCONF는 SNMP에 비해 많은 부분에서 크게 개선되었지만 네트워크 디바이스에 사용편의성을 제공하는 인터페이스를 확보하지는 못했습니다. IETF는 사용편의성을 확보하기위해 새로운 프로토콜과 데이터 모델을 개발하는 대신 NETCONF를 RESTCONF로 확장했습니다. (SSH ➔ HTTPS)
- RESTCONF는 네트워크 엔지니어와 개발자에게 쉬운 진입점을 제공하기 위해 일반적인 웹 애플리케이션 연동 방식과 동일한 REST API 호출 방식을 제공합니다.





RESTCONF	NETCONF
GET	`<get>`, `<get-config>`
POST	`<edit-config>` (operation="create")
PUT	`<edit-config>` (operation="create/replace")
PATCH	`<edit-config>` (operation="merge")
DELETE	`<edit-config>` (operation="delete")

Content	Configuration / Operational Data	XML or JSON
Operations	Actions to Take	GET, POST, PUT, PATCH, DELETE
Transport	TCP/IP Method	HTTPS

RESTCONF 서비스 제공 방법

- Cisco Catalyst 제품군의 RESTCONF 설정방법을 살펴봅시다.

Authentication of NETCONF/RESTCONF Using AAA

Enabling HTTP Services for RESTCONF

Verifying RESTCONF Configuration

```
LAB_C3850_5.51#show platform software yang-management process monitor
COMMAND          PID S    VSZ   RSS %CPU %MEM     ELAPSED
nginx          23412 S 143900 12832  0.0  0.3  7-02:14:09
nginx          23418 S 151920  7608  0.0  0.1  7-02:14:09
pubd           21737 S 352844 51848  0.0  1.3  7-02:14:30
```

```
LAB_C3850_5.51#show platform software yang-management process
confd            : Not Running
nesd             : Not Running
syncfd           : Not Running
ncsshd           : Not Running
dmiauthd         : Not Running
nginx            : Running
ndbmand          : Not Running
pubd             : Running
gnmib            : Not Running
```

- Tail-f Systems, Inc. 의 NCS ConfD 모듈 탑재 ➔ NETCONF 서비스제공
- NGINX 를 이용한 HTTP/HTTPS 서비스 제공

RESTCONF URI

- REST API 사용시 가장 중요한 것은 URI 입니다. http request/response 모델에서 전송되는 데이터 객체는 URI를 기반으로 분석이 가능합니다. RESTCONF의 독특한 측면은 개발자가 사용 방법을 배우는 데 사용할 수 있는 "API 문서" 없이, YANG 데이터 모델을 사용하여 REST API 문서를 대체할 수 있습니다.

https://⟨ADDRESS⟩/⟨ROOT⟩/data/⟨[YANG MODULE:]CONTAINER⟩/⟨LEAF⟩[?⟨OPTIONS⟩]

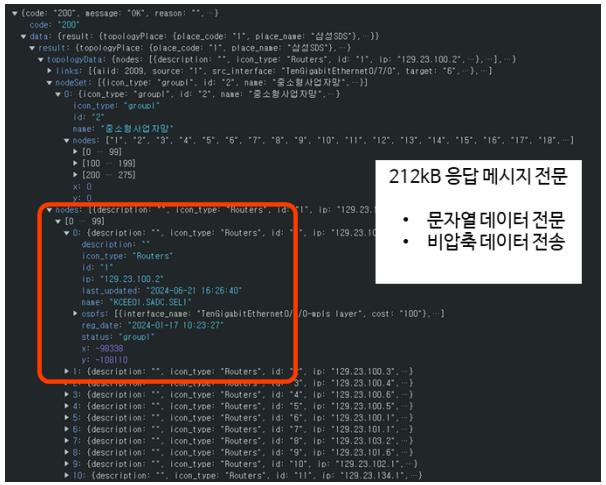
- ADDRESS – RESTCONF 에이전트를 사용할 수 있는 IP(또는 DNS 이름) 및 포트
- ROOT – RESTCONF 요청의 주요 진입점
- data – RESTCONF API 리소스 유형
  - RPC 작업에 억세스하는 데 사용되는 'operations' 리소스 유형 사용 가능
- [YANG MODULE:]CONTAINER – 사용 중인 기본 모델 컨테이너
  - Inclusion of the module name is optional.
- LEAF – 컨테이너 내의 개별 요소
- [?₩⟨OPTIONS⟩] – 쿼리 파라미터 (일부 네트워크 디바이스 지원)

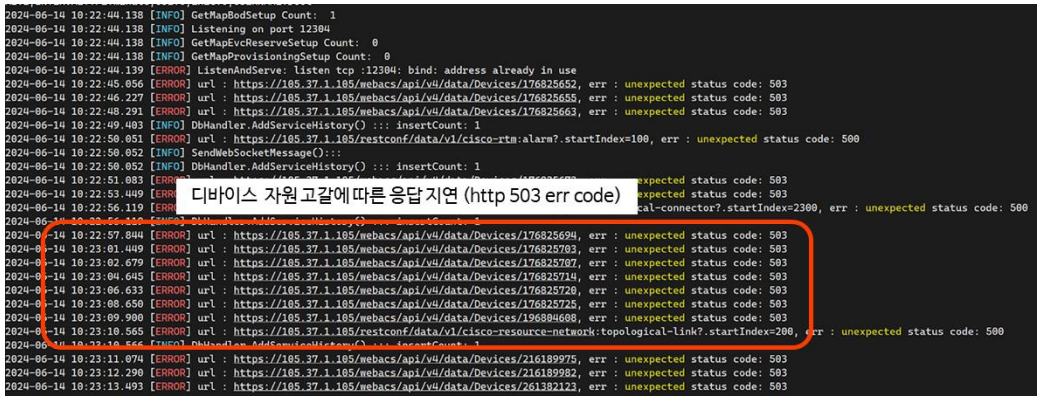
Prefix	YANG module	Reference
yang	ietf-yang-types	[RFC6991]
inet	ietf-inet-types	[RFC6991]
if	ietf-interfaces	[I-D.bjorklund-netmod-rfc7223bis]
ip	ietf-ip	[I-D.bjorklund-netmod-rfc7277bis]
rt	ietf-routing	[I-D.acee-netmod-rfc8022bis]
bfd-types	ietf-bfd-types	[I-D.ietf-bfd-yang]
isis	ietf-isis	[I-D.ietf-isis-yang-isis-cfg]
key-chain	ietf-key-chain	[RFC8177]
ospf	ietf-ospf	[I-D.ietf-ospf-yang]

```
// http://<ADDRESS>/restconf/data/ietf-interfaces:interfaces/interface=<INTERFACE NAME>?fields=name&fields=description

$ curl -k \
  -H "Authorization: Basic cm9vdDpEX1ZheSFfMTAm" \
  -H "Accept: application/yang-data+json" \
  "https://ios-xe-mgmt.cisco.com:9443/restconf/data/ietf-interfaces:interfaces/interface=GigabitEthernet1?fields=name"
```

편리한 만큼 느려지는 응답 속도

- YANG Data Model을 기반으로 하는 REST API 호출은 생소할 수 있지만, 개발자 친화적인 방법입니다. 빠르게 접근 가능하며 즉시 확인할 수 있는 장점이 있습니다. 다만, 쉬운 접근성 대비 상대적으로 높은 REST API 응답을 위한 시스템 자원 사용 및 문자열 데이터 반환에 따른 응답 속도 지연은 극복할 수 없는 디바이스 자원 고갈 및 네트워크 트래픽 증가의 원인이 됩니다.





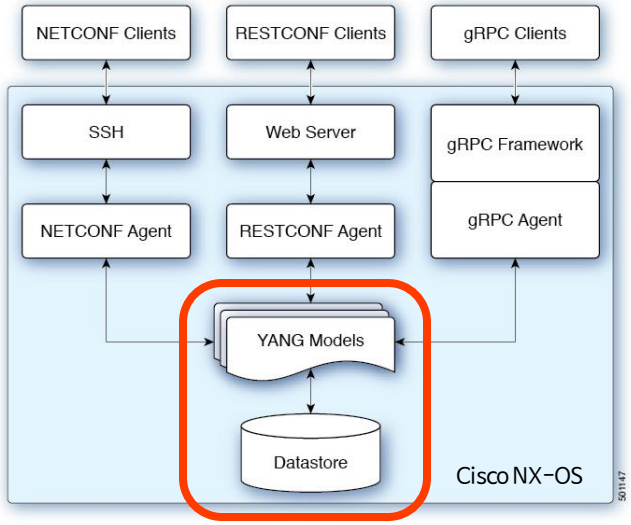
- REST API 호출 시 수 밀리세컨드에서 수 초 소요 ➔ 네트워크 디바이스 리소스 고갈
  - “시스템 요청 ➔ 디바이스 인증 및 수락 ➔ 데이터 수집 ➔ 데이터 반환”에 따른 서비스 사이클 개선 필요

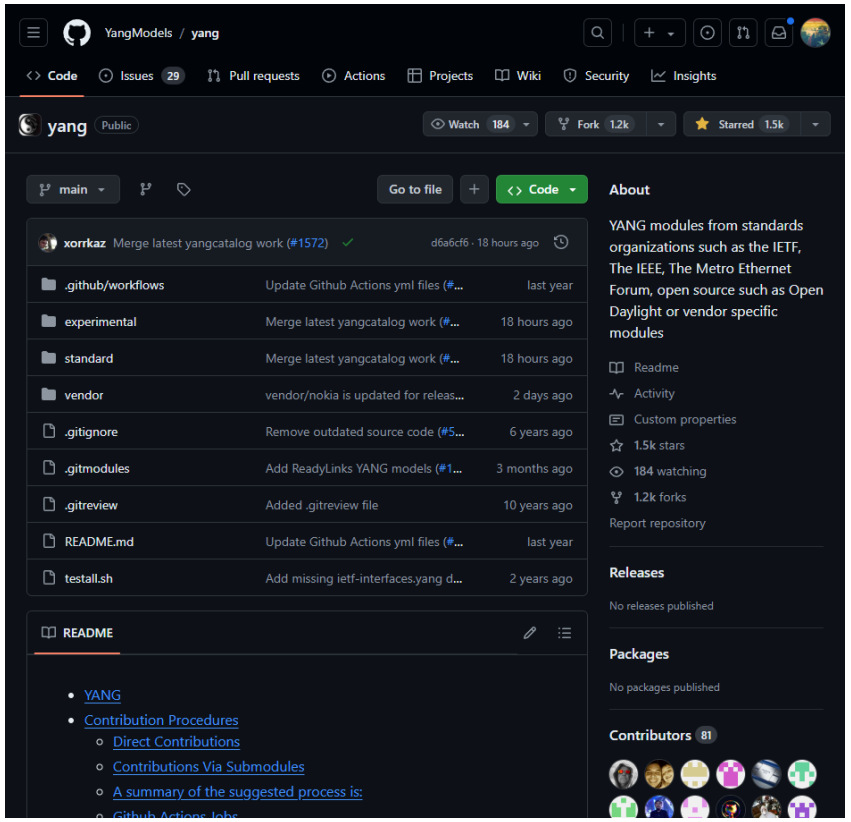
- REST API 응답 메시지 전문 용량 증가 (수 B에서 수백 kB) ➔ 네트워크 트래픽 증가
  - 문자열 데이터 전문 및 비압축 데이터 전송
  - http/1.1 의 블로킹 현상 해소, http/2 적용에 따른 바이너리 헤더 및 데이터 전달 개선
  - 네트워크 디바이스와 시스템이 상호 인지하는 데이터 포맷 필요 ➔ key/value 타입의 정규화된 프로토콜 필요

YANG Data Model

- 데이터 모델은 단순히 “무언가”를 설명하기 위해 잘 정의된 방법입니다. YANG 데이터 모델은 NETCONF 사용을 위해 필요한 데이터 모델을 정의하고 있습니다. YANG 데이터 모델은 네트워크 디바이스의 원격제어를 위해 외부에서 확인할 수 있는 데이터의 구조, 구문 및 의미를 명확하게 정의하고 있으며, 시스템과 클라이언트 간의 상호 작용의 완전성과 일관성을 보장합니다.

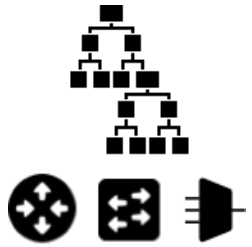
```
module: Cisco-IOS-XE-native
  +--rw native
     +--rw default
     |  +--rw crypto
     |     +--rw ikev2
     |        +--rw proposal?                empty
     |        +--rw policy?                  empty
     +--rw bfd
     +--rw version?                          string
     +--rw stackwise-virtual!
     +--rw boot-start-marker?                empty
     +--rw boot
     |  +--rw system
     |     +--rw tftp-path?                  string
     |     +--rw tftp?                       string
     |     +--rw bootfile
     |     |  +--rw filename-list*           [filename]
     |     |     +--rw filename              string
     |     +--rw flash
     |        +--rw flash-list*              [flash-leaf]
     |           +--rw flash-leaf            string
     +--rw boot-end-marker?                  empty

Edited for simplicity and brevity
```





OpenConfig

- YANG 모델을 활용한 OpenConfig는 네트워크 디바이스 관리를 위한 공급업체 및 사업자, 사용자들이 협력하는 독립적인 공통 소프트웨어 계층을 정의하고 구현합니다. OpenConfig는 네트워크 서비스사업자, 장비 공급업체 및 더 넓은 커뮤니티의 기여를 통해 오픈 소스 프로젝트로 운영되며 새로운 규정준수를 위한 기술개발을 선도하고 있습니다.



Common data models

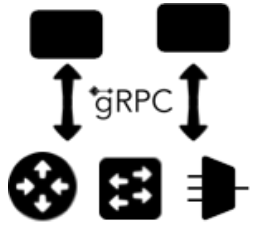
공통 데이터 모델

- 다양한 네트워킹 사용 사례에서 공급업체 중립적인 관리를 위해 사용자가 설계한 일관되고 일관된 데이터 모델입니다.

Streaming telemetry

스트리밍 텔레매트리

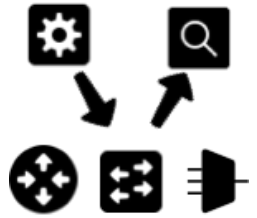
- 스트리밍 원격 분석은 OpenConfig 모델을 기반으로 네트워크 장치를 효율적이고 정확하게 모니터링하기 위한 구독 기반 모델입니다.



Management protocols

관리 프토로콜

- 분산 서비스를 위해 구축된 최신의 안전한 RPC 프레임워크인 gRPC를 기반으로 하는 기기 관리 및 제어 프로토콜입니다.



Testing and compliance

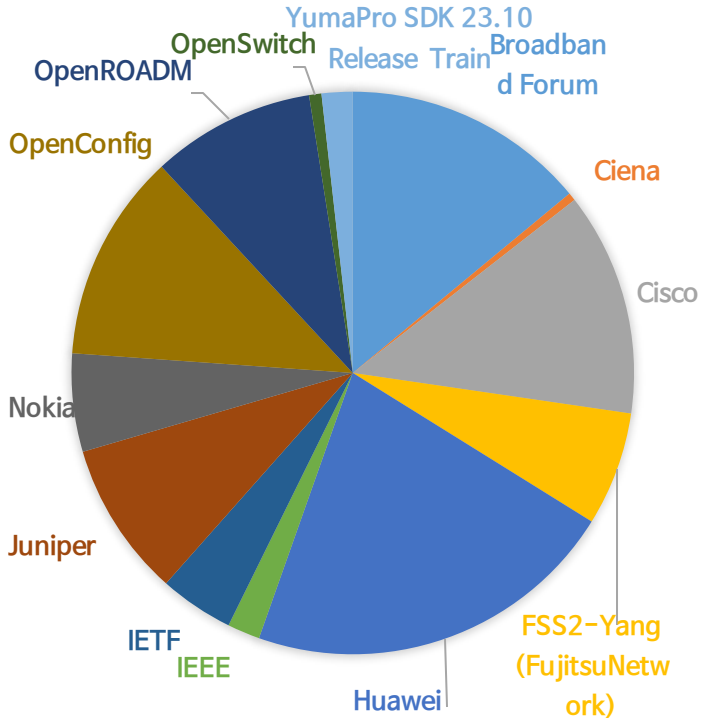
테스트 및 규정준수

- 공급업체에 독립적인 자동화를 통해 OpenConfig 구현의 규정 준수 테스트를 간소화하여 비즈니스를 가속화합니다.

Cisco, Juniper, Ciena, Nokia …

- 브로드밴드포럼, IEEE, IETF, OpenSwitch, OpenROADM 등 다양한 기관에서 OpenConfig와 같은 YANG Data Model 기여를 주도하고 있으며, Cisco, Ciena, Huawei, Juniper, Nokia 등 다양한 네트워크디바이스제조사에서 자사 제품에 YANG Data Model을 적용하고 있습니다.

제조사	Subtree	Count
Broadband Forum	• /standard	613
Ciena	• /vendor/ciena	20
Cisco	• /vendor/cisco	563
FSS2-Yang (FujitsuNetwork)	• *	287
Huawei	• /network-router	944
IEEE	• /standard/ieee	82
IETF	• /standard/ietf • /experimental/ietf-extracted-YANG-modules	187
Juniper	• /21.3/21.3R1	391
Nokia	• /latest_sros_24.3	247
OpenConfig	• /release/models	525
OpenROADM	• /model	412
OpenSwitch	• /yang-models	31
YumaPro SDK 23.10 Release Train	• /netconfcentral • /yumaworks	78
		4,380



- Broadband Forum, IEEE, IETF, OpenConfig, OpenROADM, OpenSwitch ➔ 1,850
- Ciena, Cisco, Huawei, Juniper, Nokia ➔ 2,165

효율화, 구조화, 정규화

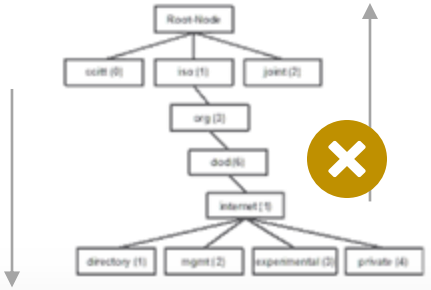
- 네트워크 엔지니어는 보통 5분에서 30분 간격으로 네트워크에서 데이터를 폴링합니다. 신중한 튜닝과 노하우, 테스트를 통해 그 간격을 1분으로 줄일 수 있습니다. 하지만 오늘날의 속도와 규모를 고려할 때 이 정도로도 중요한 네트워크 이벤트를 포착하기에 충분하지 않습니다.

어떻게 하면 디바이스에서 최대한 많은 데이터를 사용하기 쉬운 방식으로 최대한 빨리 가져올 수 있을까?

효율화
Streaming

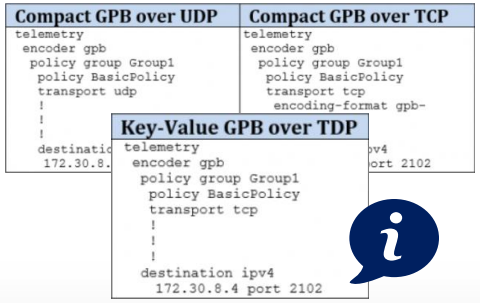
- 네트워크모니터링은 일정한 간격의 주기적인 데이터 필요 ➔ SNMP와 같은 폴링 메커니즘 사용
- 네트워크 디바이스에서 일정주기의 데이터를 전송하는 푸시 메커니즘 고안 ➔ 스트리밍 메커니즘으로 발전

구조화
Yang Data Model



- 스트리밍 데이터의 오버스펙을 제거하기 위한 합리적인 구조화 요구 ➔ 모델 기반
- 네트워킹 업계의 데이터 모델링 언어 ➔ YANG
  - IEEE/IETF, OpenConfig, Vendor Native 등

정규화
kv GPB



- 소프트웨어 애플리케이션 간의 데이터 전송 요구 ➔ 정규화된 인코딩 기술 채택
  - JSON, key/value Google 프로토콜 버퍼 (GPB)
- 간편한 데이터 조작 및 분석을 위한 오픈소스 에코시스템

Model Driven Telemetry

ICMP부터 Telemetry까지

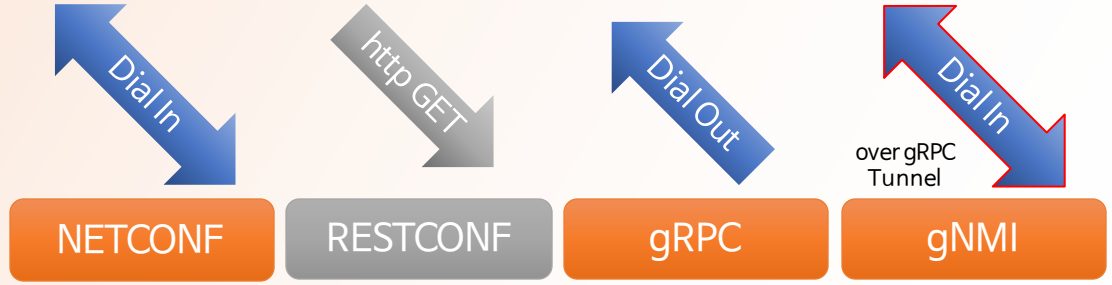
GOODUS

MDT, Model Driven Telemetry

- 다양한 현업의 필요성에 의해서 네트워크는 정규화된 YANG 데이터 모델을 NETCONF 프로토콜로 푸시하여 구성됩니다. YANG 데이터 모델 컨피그가 네트워크에 배포되었다고 모든 구성이 완벽한 것은 아닙니다. 여기에는 서비스 모니터링을 위한 텔레매트리 매커니즘도 구성되어야 합니다. 모델기반 텔레매트리는 실시간으로 중요 데이터를 수집하고 측정할 수 있으며, 대부분의 네트워크 운영 문제에 대한 해결방안을 제시할 수 있습니다.

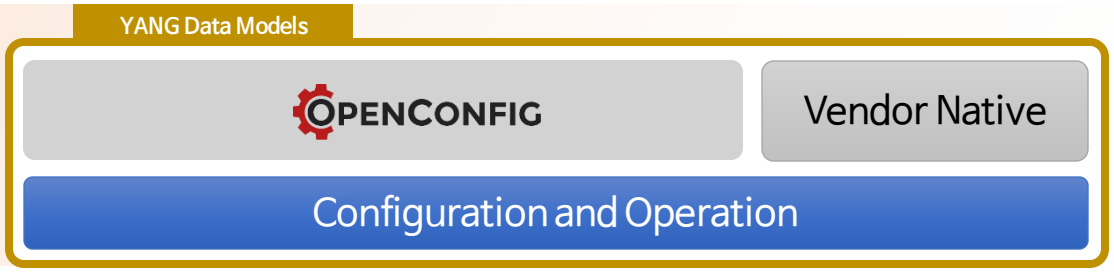
- 모델기반 텔레매트리는 네트워킹 디바이스에서 지원하는 구조화된 데이터 모델을 활용하고 해당 데이터 모델에 정의된 중요 데이터를 제공함으로써 새로운 인프라스트럭처 자동화 스택을 구성합니다.
- 유연한 데이터 모델 구조는 자동화 프로세스를 위한 구성 도구로써 이점을 제공하며 특정 인코딩 형식 및 전송 프로토콜과 결합되어 모델기반 텔레매트리를 네트워크 분석을 위한 완벽한 솔루션으로 만들어 줍니다.

XML, JSON, proto and kvGPB encoding



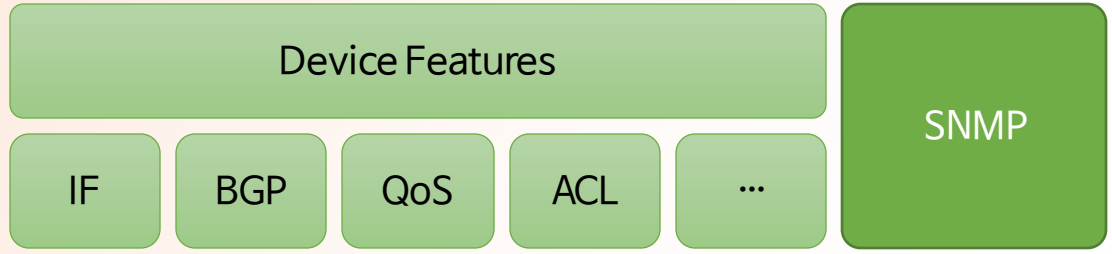
- 텔레매트리는 네트워크에서 수집된 표준 데이터로 산업 전반에 걸쳐 균일하게 형성되었으며, 네트워크 엔지니어가 하나의 공통 네트워크 관리 시스템, 프로세스 및 애플리케이션을 사용하여 멀티 벤더 네트워크를 관리할 수 있도록 지원합니다.

Consistent YANG data models between interfaces



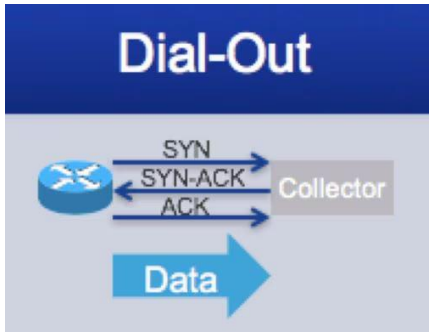
- 최근 데이터 모델의 표준이 된 정규화된 YANG 데이터 모델은 기존 SNMP MIB, OID 계층 구조를 수용하며 네트워크 프로그래머빌리티 스택에서 네트워크를 통해 효율적인 데이터 세트를 형성하고 전송하는데 사용됩니다.

On-Change event and time-based publication options

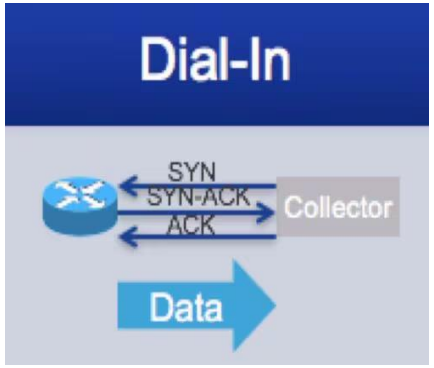


Model Driven Telemetry Configuration

- 네트워크 엔지니어는 효율적인 서비스 환경 구성을 위해 전송방식(gRPC)과 인코딩(kv GPB)의 이점을 이해하고 세션(Dial-In/Out)을 구성해야 합니다. 일반적으로 탤레매트리 세션관리는 네트워크 디바이스가 어플리케이션으로 Dial-Out 하거나 어플리케이션이 네트워크 디바이스로 Dial-In 하여 연결, 유지합니다.



- Dial-Out 모드에서 네트워크 디바이스는 어플리케이션에 구독을 설정한 센서 그룹의 데이터를 TCP 세션으로 전송합니다. ➔ Push
  - 전송 옵션에 대한 더 넓은 유연성
  - 인바운드 관리 트래픽을 위한 별도의 서비스(포트) 불필요
  - 애니캐스트 및 로드 밸런싱



- Dial-In 모드에서 어플리케이션은 네트워크 디바이스에 접속하여 동적으로 구독을 설정하거나, 다양한 센서 정보를 수신합니다. (네트워크 디바이스 == 서버, 어플리케이션 == 리시버 (!= 클라이언트))
  - 구성 및 스트리밍을 위한 단일 채널
  - 네트워크 디바이스 포트 수신(listen)
  - 일시적 연결
  - 현재 gRPC/gNMI만 사용 가능

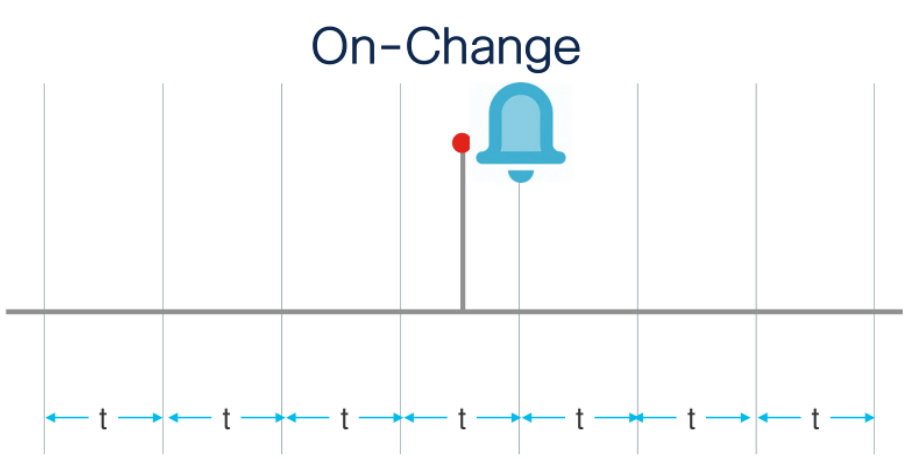
Model Driven Telemetry Interface Comparison

- 네트워크 아키텍처, 보안 태세 및 정책, YANG 데이터 모듈, 도구 및 언어 기본 설정, 표준, 소프트웨어 버전은 다양한 MDT 인터페이스를 활용할 때 고려해야 할 몇 가지 사항입니다.

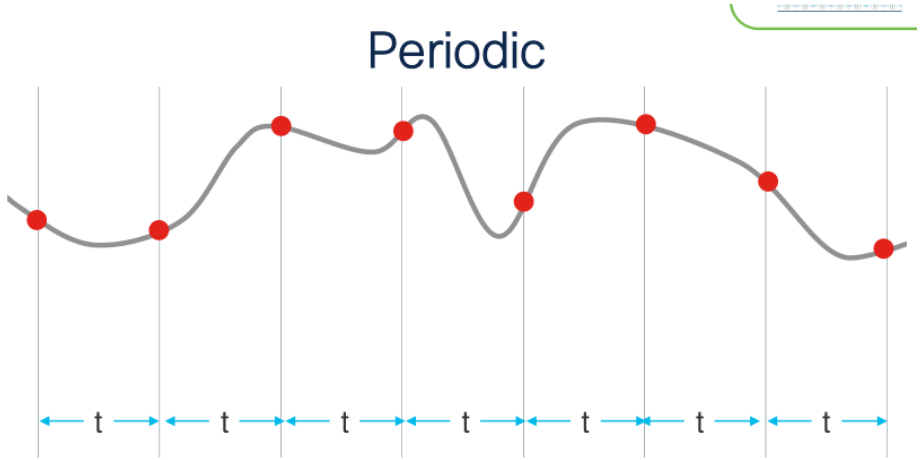
	NECTCONF	gRPC (Dial-Out)	gNMI
Telemetry Direction	Dial-In IOS XE is Server	Dial-Out IOS XE is Client	Dial-In, IOS XE is Server Dial-Out, gRPC Tunnel
Configuration	Dynamic per Session	Static per Configuration	Dynamic per Session
Telemetry Collector	Client	Server	Client
Encoding	XML	KB GPB	JSON_IETF + PROTO
Security	SSH + PKI Certificate or Password	mTLS or plain-text	mTLS Certificates - mTLS Cert only - mTLS Cert + user/pass Authentication
Transport Protocol	SSH	HTTP/2	HTTP/2
Data Models	YANG	YANG	YANG

Model Driven Telemetry Publication

- 실시간 성능 및 구성 데이터 수집이 가능한 모델기반 텔레매트리 퍼블리싱은 “On-Change” 타입과 “Periodic” 타입으로 구분되어 스트리밍 텔레매트리 매커니즘을 구조화하여 이벤트 알림, 상태 및 구성 알림, 주기적 퍼블리싱 등 다양한 데이터 스트림을 생성합니다.



- Feature Model “On-Change” Notifications
- Event Notifications (failed login, optic fault, etc.)
- State and Configuration



- Feature Model “Periodic” Notifications
- Time based publication
- Minimum interval 1sec

Ansible, Terraform

ICMP부터 Telemetry까지

GOODUS

Ansible, Terraform

- Ansible 및 Terraform은 IT 환경 자동화를 위해 코드형 인프라(Infrastructure as Code, IaC) 접근 방식을 수용한 오픈소스 기반의 자동화 제품입니다. 각 제품의 특장점은 서로 다르지만, 중요한 점은 Ansible 과 Terraform 역시 NETCONF와 RESTCONF를 통해 네트워크 인프라의 자동화를 추구한다는 점 입니다.

Ansible is an open-source, Infrastructure as Code (IaC) Software suite. It is agentless, meaning there is no installation and no requirements on the target device, other than having an accessible API or interface.

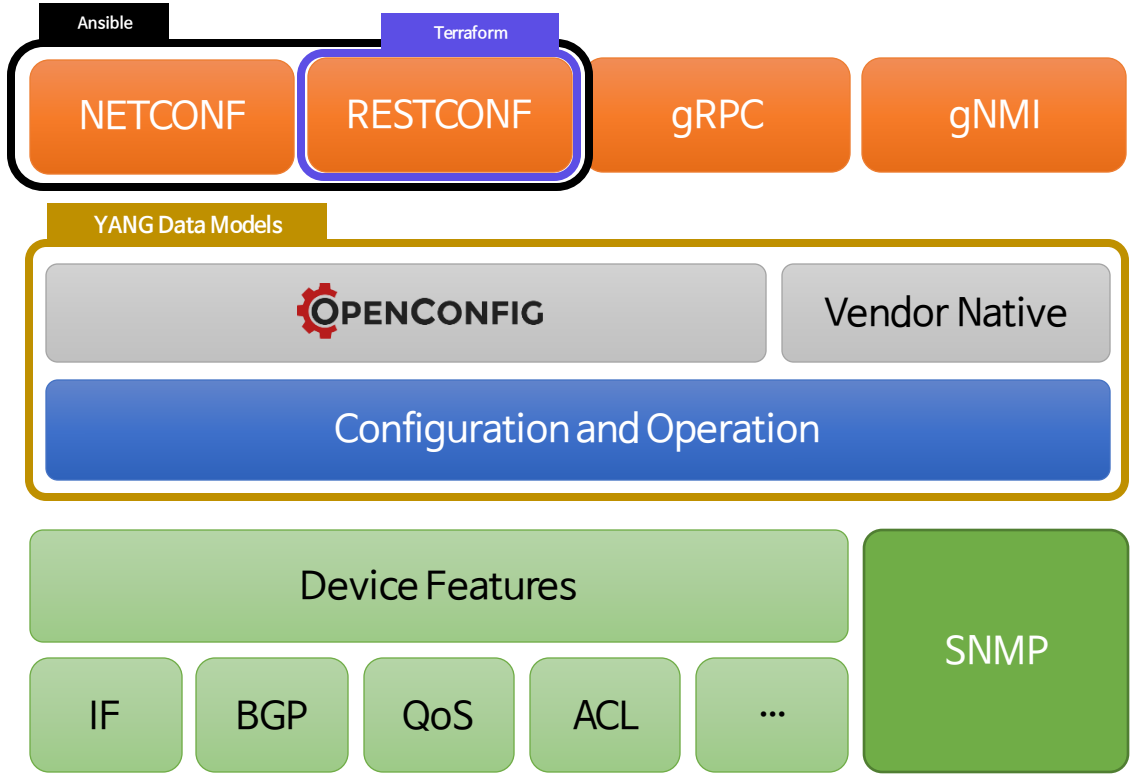
- minimal in nature and provides a secure and reliable way to interact with remote devices
- highly adaptable and commonly used with other automation tools to accomplish complex workflows.

Infrastructure as Code (IaC) Software Tool providing a consistent CLI workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.

- Cloud Native Tooling circa 2014 from HashiCorp
- Agentless, single binary file
- Zero server-side dependencies

ANSIBLE

HashiCorp Terraform



Goodus Network Experience Insights

Goodus Network Experience Insights

Enterprise & Cloud Infrastructure Network Operations & Management, Monitoring & Management

Xpert Network Platform™

Streaming Data Collection, Infra-to-service Correlation, Visibility, Autonomous

Cloud Metering & Service Portal	Network O&M (Operation & Maintenance)				Network M/M System (Monitoring & Management)					Automation, Provisioning	Enterprise AI	Cisco Integration
Cloud Network Portal	Network Command & Utilities	ICMP/IGMP, SNMP/Syslog, Trap	NETCONF/YANG RESTCONF	Telemetry, gNMI/gNOI	Fault Management	Config Management	Account Management	Performance Management	Security Management	APC, NetCheckUp Auto Provisioning Center Config Validation	Enterprise AI Anomaly Detection Adaptive Threshold AI Assistant (sLLM)	Cisco Catalyst Center Managed SVC
G-Cloud Viewer										Travis Cisco EPNM based T-SDN Controller w/ Nokia, HUAWEI		

Samsung Cloud Platform, aws, Azure, cisco, cisco Meraki, ARISTA, HPE aruba networking, Hewlett Packard Enterprise, radware alteon, Extreme networks, DELL Technologies, A10, f5, juniper networks, NETCONF RESTCONF, YANG, OPENCONFIG, NVIDIA, Microsoft, CISCO INTERSIGHT, ThousandEyes

Appendix

제 37회 네트워크 전문가 따라잡기 N.EX.T

References

- FCAPS - https://www.slideserve.com/totie/fcaps
- Application of Bayesian Networks for Autonomic Network Management - https://www.researchgate.net/publication/258163873_Application_of_Bayesian_Networks_for_Autonomic_Network_Management
- ITIL&FCAPS - NETWORK MANAGEMENT FUNDAMENTALS - http://www.codrm.eu/conferences/2012/34_Barbu.pdf
- Introducao aos conceitos de programabilidade de infraestruturas de redes - https://wiki.brasilpeeringforum.org/w/Introducao_aos_conceitos_de_programabilidade_de_infraestruturas_de_redes
- Essential SNMP, 2nd Edition - https://www.oreilly.com/library/view/essential-snmp-2nd/0596008406/
- Net-SNMP - https://net-snmp.sourceforge.io/
- 네트워크 정보 수집 프로토콜의 모든 것 (SNMP, RMON, ICMP, Syslog) - https://www.brainz.co.kr/tech-story/view/id/251#u
- 고전 돌아보기, C10K 문제 (C10K Problem) - https://oliveyoung.tech/blog/2023-10-02/c10-problem/
- Cisco's onePK Part 1: Introduction - https://blogs.cisco.com/security/ciscos-onepk-part-1-introduction
- Network Virtualization: a next generation modular platform for the data center virtual network - https://bradhedlund.com/2013/01/28/network-virtualization-a-next-generation-modular-platform-for-the-virtual-network/
- 차세대 네트워킹 시대를 견인하는 SDN과 NFV - https://www.spri.kr/posts/view/21671?code=industry_trend
- An architect's guide to Network Programmability - https://www.redhat.com/en/blog/architects-guide-network-programmability
- NETCONF에 대해 - https://bumday.tistory.com/129
- Introduction to Model Driven Programmability - https://developer.cisco.com/learning/tracks/EN-Networking-v0/intro-device-level-interfaces/
- http/2 프로토콜 적용하기 - https://tecoble.techcourse.co.kr/post/2021-09-20-http2/
- Cisco YANG Suite : https://developer.cisco.com/yangsuite/
- YANG Data Model Github Repository : https://github.com/YangModels/yang
- OpenConfig : https://www.openconfig.net/
- Netconf Central : https://www.netconfcentral.org/
- Programmability Configuration Guide, Cisco IOS XE Cupertino 17.9.x : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/179/b_179_programmability_cg/m_179_prog_restconf.html
- Tail-f Systems : https://www.youtube.com/@TailfSystems

감사합니다

제 37회 네트워크 전문가 따라잡기 N.EX.T

GOODUS