Human Factors In Improving Operations Reliability

Carl Colwill Principal, Information Assurance BT Security, BT
carl.colwill@bt.com

Alpha Chen Senior Reliability Engineer, Huawei
chenlifu@huawei.com

Presenter:
Himanshu Pant Senior Manager, Huawei
hpant@huawei.com

Abstract

- Human factor caused service outages are a big percentage (like more than 30%) of the network outages
- It's a major concern for carriers and causes big revenue-loss. Especially for the future All-IP network, this problem is becoming increasingly serious.
- This presentation will discuss the methods and technologies for preventing human factor error. It will cover the **processes, tools and managements issues**, etc. which Huawei and BT have researched and implemented.

General Introduction — An unending saga

- In **1998, a misconfigured critical Internet database server** incorrectly referred all queries for Internet machine names ending in \.net" to the wrong secondary database server. As a result, a majority of connections to \.net" Internet **web servers and other end stations failed** for a period of several hours.
- In **2006**, a technical support engineer **mistakenly connected two routers with different versions** during the IP carrier network cut over. The older version router advertise its static routing information to a new target network, and formed a routing loop, resulting in the **loss of service of softswitch equipment in four big cities**.
- In **2006**, during network inspection, a technician detected some redundant data. He **accidentally deleted the VLAN services** instead of clearing the redundant data. The operation error resulted **loss of Internet connections** for many user's across several cities.
- In **2007**, in course of routine maintenance, an American service-provider **deleted an active optical fiber without first configuring fiber protection**. The mistake resulted in Internet **services being unavailable for nearly 2 hours**.
- In **2009**, a **hacker attacked the Twitter website** and put calumnious words and pictures on more than 30 famous users' blog webpages through dictionary attack. The hacker said that the website's weak **password management was the "culprit".**

General Introduction — Human errors are becoming increasingly serious

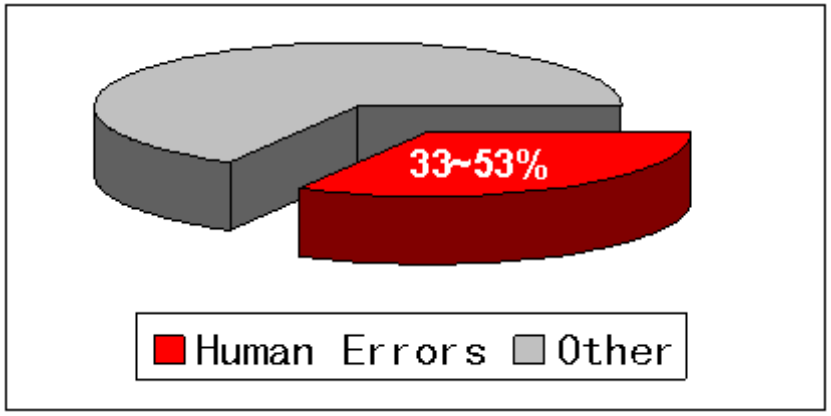


Figure 1. From FCC

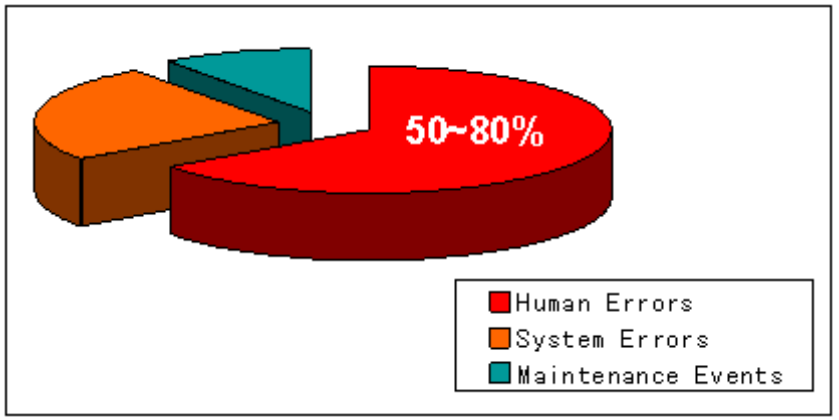
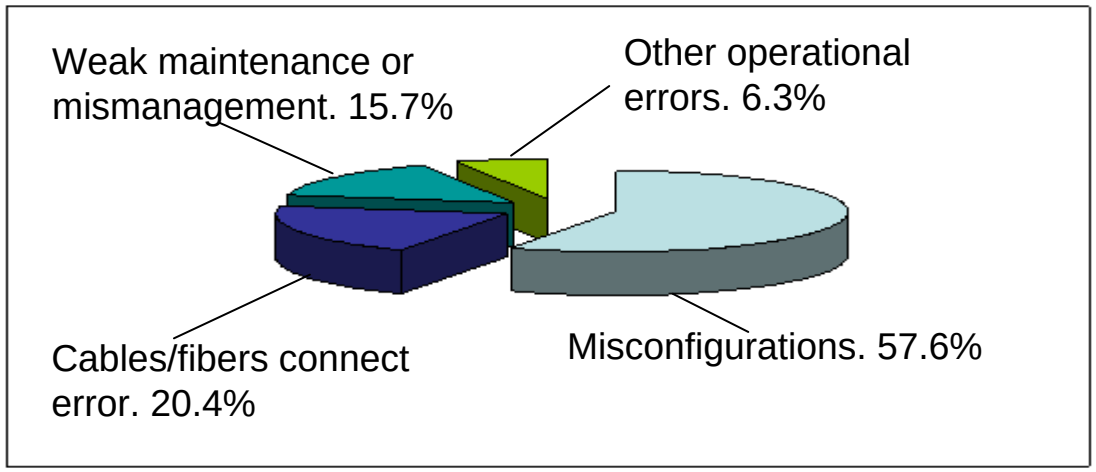


Figure 2. From research organization(2006)

- The researches from FCC and other organization indicate that **human errors are becoming increasingly serious**.
- Some top-tier providers said also that **human errors are the root causes of most network interrupt and security threats**.

General Introduction — Misconfigurations are the main category of human errors



- **Human errors can be grouped into follow categories (*):**
  - **Misconfigurations.** These include **failure to configure protection** resulting in service-outages when active fiber is broken, **accidental deletion of active services**, **inconsistent parameter** (such as port work mode, MTU) **configuration**.
  - **Cables/fibers connect error.** Examples would be **cables/fibers plugged-in/pulled-out from incorrect ports**, touching the **cables/fibers** unintentionally so that they **fall off or become loose**.
  - **Poor maintenance or mismanagement.** Such as **closing the air-conditioning** so that temperature becomes too high, cleaning dustproof nets or fans incorrectly or not in time.
  - **Other operational errors.** These include **plugging boards into incorrect slots**.

(*) Analysis of HUAWEI's carrier network products field data.

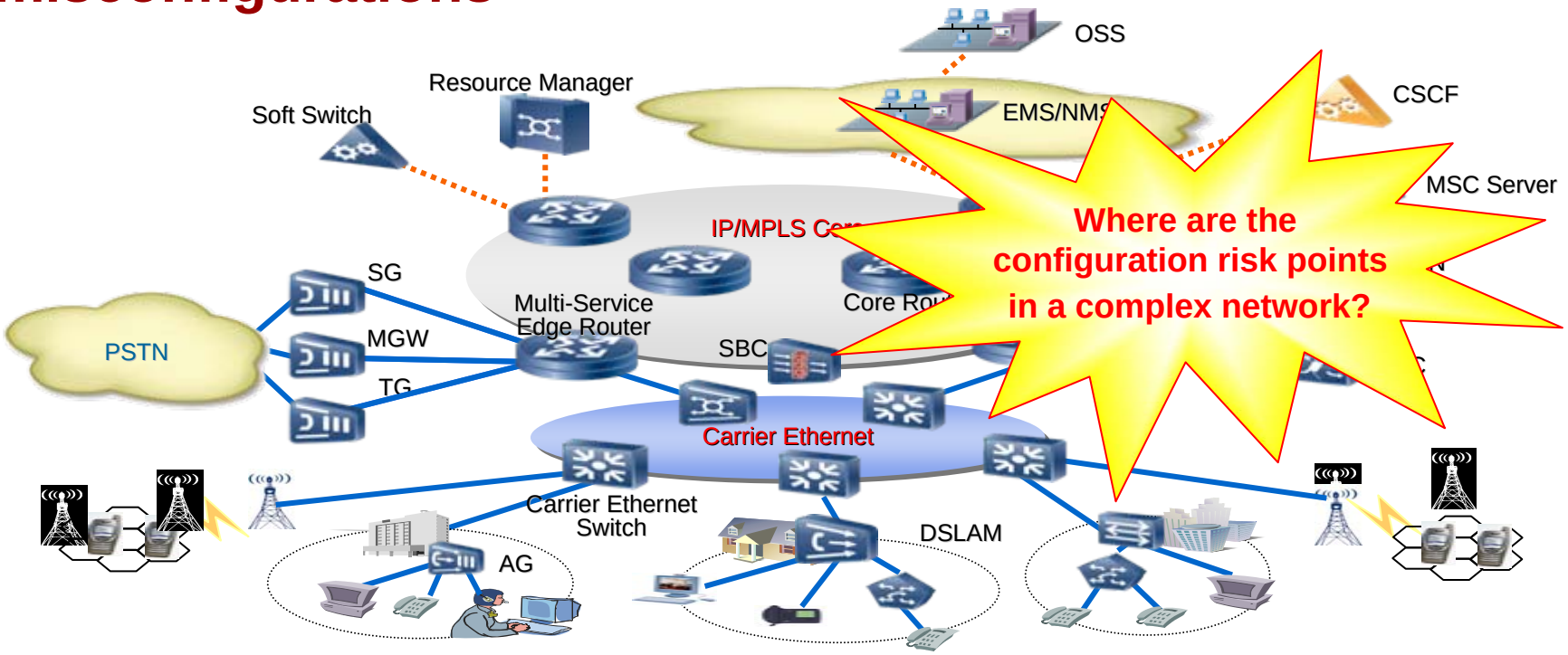
General Introduction — Root causes of misconfigurations

- **Most misconfigurations are unintentional – threaten network security due to lack of caution**
  - Operator erroneously believes the configurations are right.
  - Operator is not acquainted enough with configuration and so that mistakes.

  configuration complexity is the root cause of misconfigurations

- **Some misconfigurations are intentional – disregard network security**
  - Unauthorized.
  - Ignore service-affecting alarm.

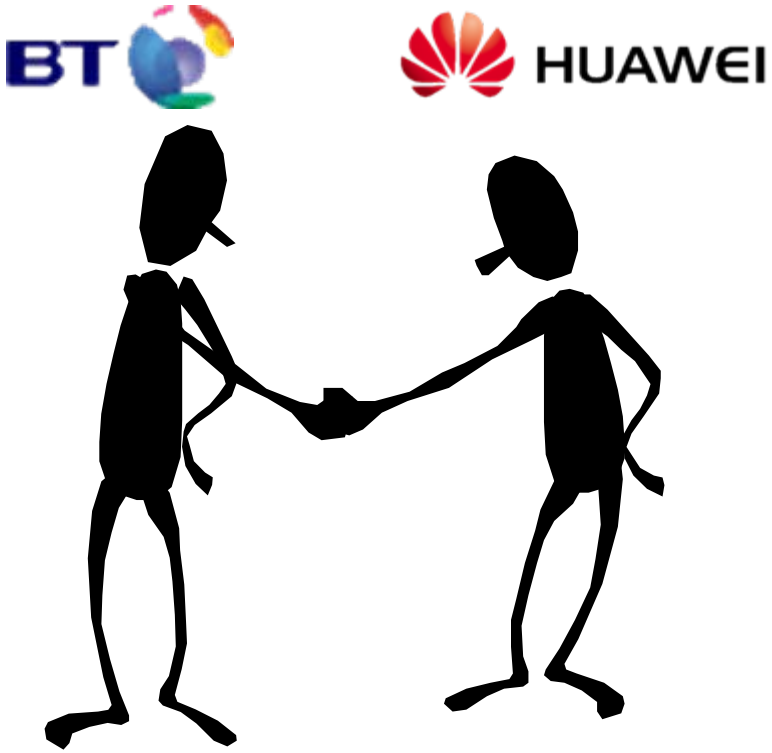
General Introduction — Complexity is the root cause of misconfigurations



- The **increasing complexity** in the networks and services **challenges the network's management, operations, and security**.
  - Multiple technologies and multi-vendor devices in the same network
  - Many services and applications converge in a same network
  - Management of many medias and services
  - E2E services security, availability, QoS and SLAs
  - … …

Solution – Misconfiguration is a complex area and requires close co-operation between vendor and customer

- Understand how the customer's procedures and processes may be affected
- Understand device and solutions limitations (taking into account agreed minimum levels of security)
- Integrate appropriate vendor, customer and international best practise recommendations
- Security functions should look for problems throughout the life of the solution and work together to mitigate and fix issues affecting the security of a solution
- …



Solution – Service providers' strategies and practices

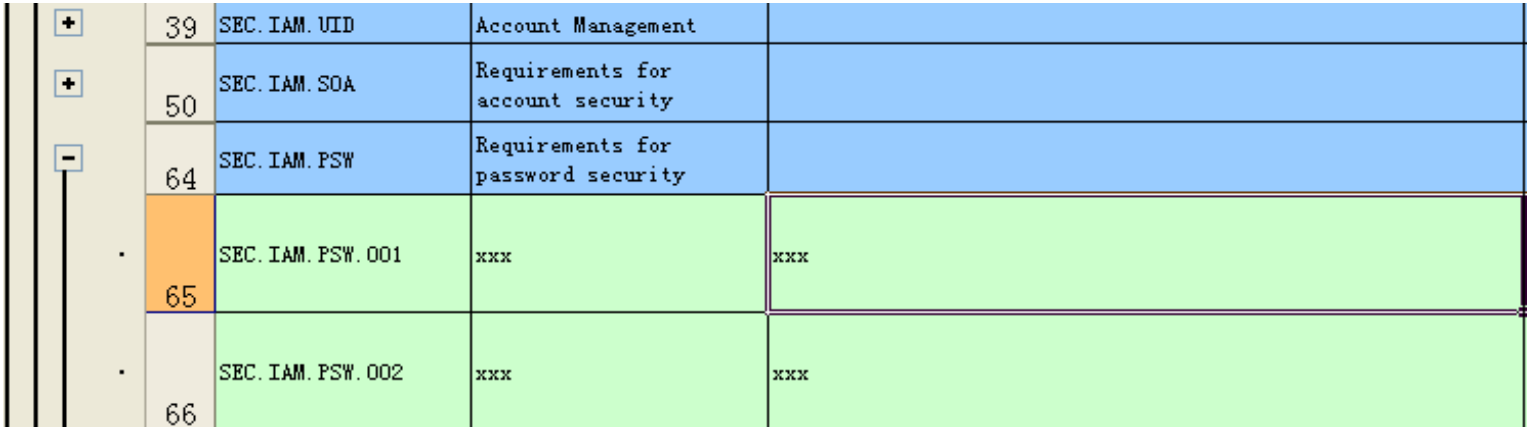
- **Providers should emphasize supervision and training**
- **Organize training; especially for new technicians**
  - **FCC "Best Practices",** such as:
    - Use of a detailed Method of Procedure
    - Use of a maintenance window
    - "Ask Yourself"
    - Maintain the awareness and sensitivity of the technician
    - "Approval for Use"
    - …
  - **Organizational Best Practices**
  - **Knowledge of the network topologies, elements and services**
    - Plan and configure the networks reasonably
  - **Inspect/monitor the configurations and networks-states**
    - Periodically and handle faults in time
  - …

Solution – Vendors' strategies and practices

- **Vendors should employ misconfiguration-prevention techniques**
  - **Human-Centred Design**
    - The standard documents, such as GR2914, ISO9241, IEC62508, present the requirements or methods of Human-Centred Design (HCD) or User-Centered Design (UCD)
  - Understand **user operations**
    - Automation configurations
    - One-key design
    - Batch configurations
    - Wizard
  - **Prevent error input** from becoming a problem
    - Actively prevent misconfigurations
    - Build security into the solution such as authorization mechanisms
    - Protection mechanism for misconfigurations
  - **Rapid error isolation** and recovery
    - Recording mechanisms, such as log "**3W"** - **W**ho did the action, and **W**hen, and **W**hat they did
  - **Tools for inspecting/monitoring** the configurations and states of the networks
  - **Tested in the labs**
  - **Quality documentation** and on-product helps

HUAWEI's practices – An example

- Built security into the solution based on "security requirement baseline", such as the following:



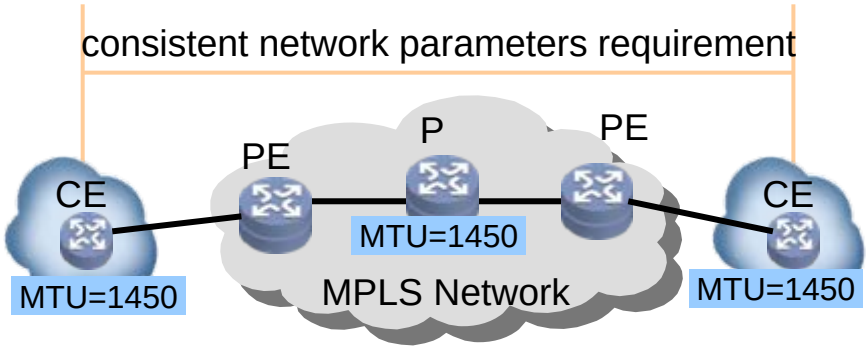
39 SEC.IAM.UID	Account Management	
50 SEC.IAM.SOA	Requirements for account security	
64 SEC.IAM.PSW	Requirements for password security	
65 SEC.IAM.PSW.001	xxx	xxx
66 SEC.IAM.PSW.002	xxx	xxx

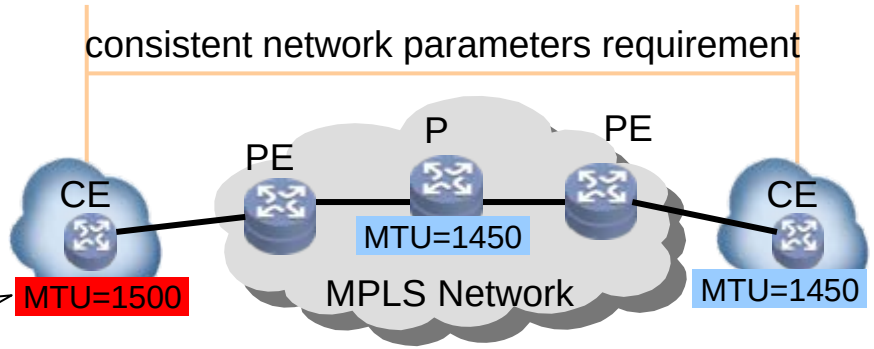
- Recording mechanisms to log "3W" – Who, When, What:

```
%Feb  6 2009 15:00:10 NE40E-X3 %%01SHELL/5/CMDRECORD(l)[2909]:Record command information. (Task=HS2M,
Ip=**, User=**, Command="igmp enable")
%Feb  6 2009 15:00:10 NE40E-X3 %%01SHELL/5/CMDRECORD(l)[2910]:Record command information. (Task=HS2M,
Ip=**, User=**, Command="igmp on-demand")
%Feb  6 2009 15:00:10 NE40E-X3 %%01SHELL/5/CMDRECORD(l)[2911]:Record command information. (Task=HS2M,
Ip=**, User=**, Command="igmp ssm-mapping enable")
```

HUAWEI's practices – Design to identify configuration risk points

- **Configuration correlation analysis – clarifies complicated configurations**
  - Ensures **consistency** of configurations between services/functions
  - Clarifies **dependencies** between services/functions configurations
  - Points out **configuration-conflicts** between services/functions
  - Identifies **prohibited or required configurations** for services/functions
- **Configuration actions analysis - find out which actions result in misconfigurations easily**
  - What user needs to do - configure entry
  - What user can do - possible user inputs
  - List the impact of erroneous inputs

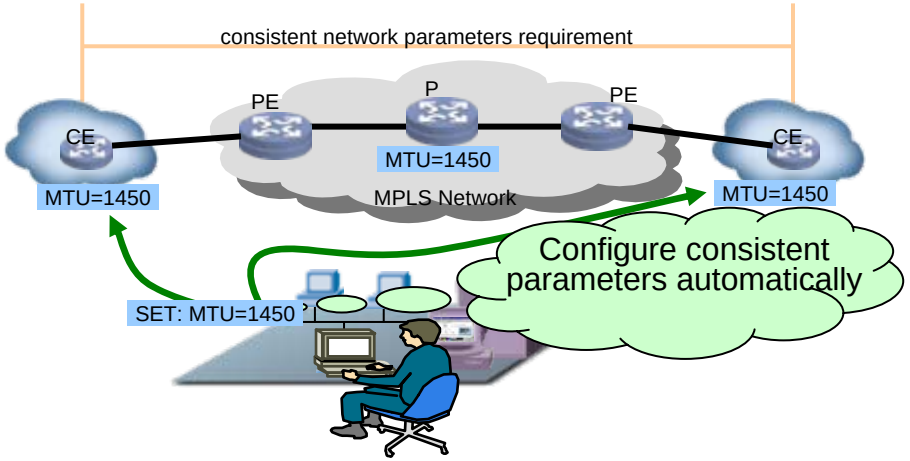


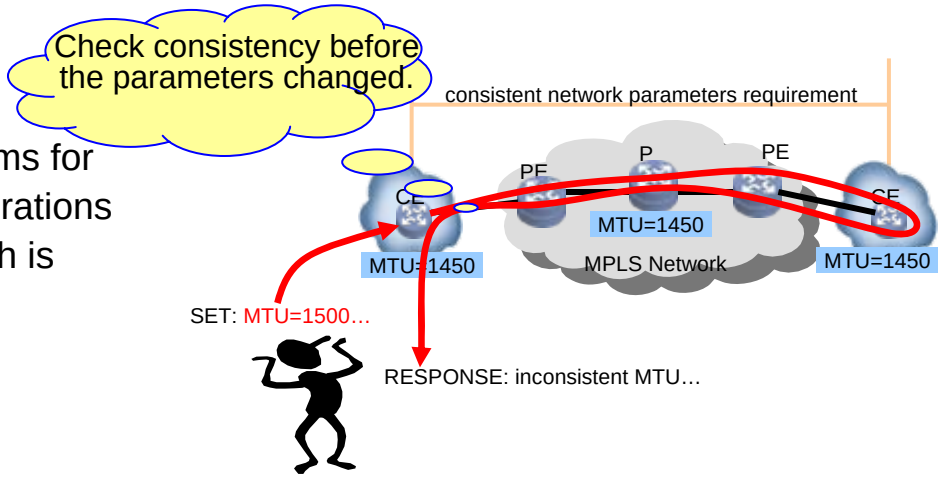


1.What user need to do - configure consistent MTU for connection
2. What user can do – user can input any MTU value
3. The input impact the purpose – input of inconsistent MTU will break the connection

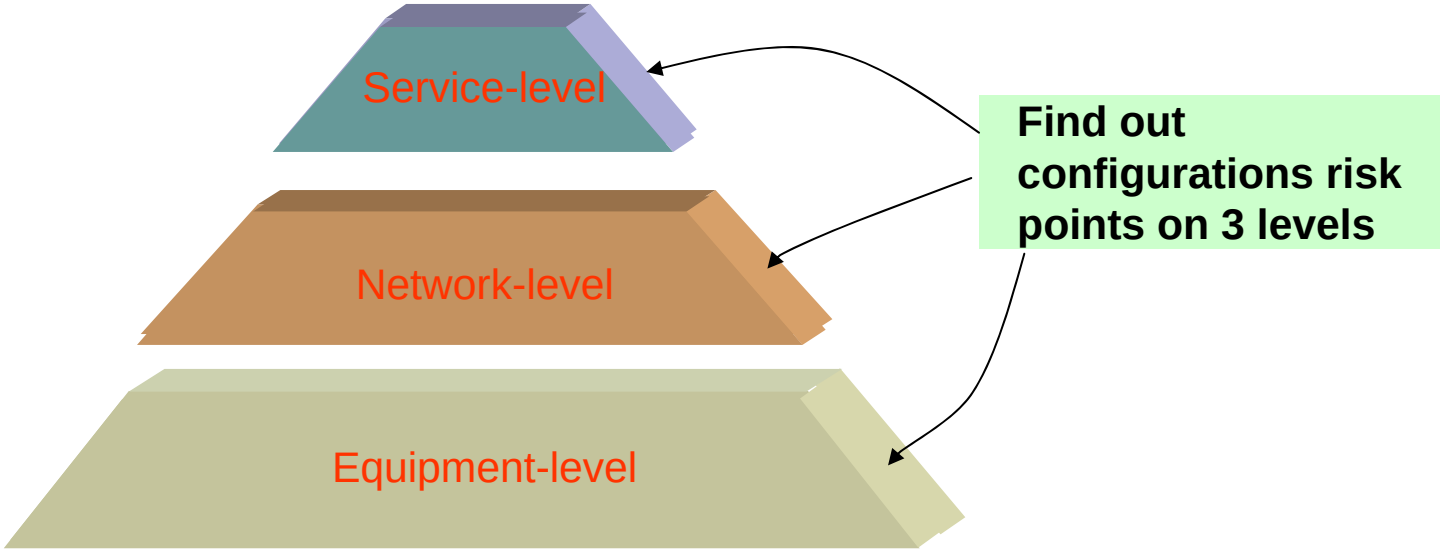
HUAWEI's research and practices – Prevent misconfigurations

- **Reduce configuration risk points**
  - Automatic configuration
  - One-key design
- **Prevent misconfigurations at risk points**
  - Human-Centred Design to prevent misconfigurations，refer to GR2914, ISO9241, IEC62508.
  - Detect, alarm and prevent misconfigurations.
  - Correction or protection mechanisms for misconfigurations, such as configurations roll back or services protection path is established.
  - Tools to check misconfigurations



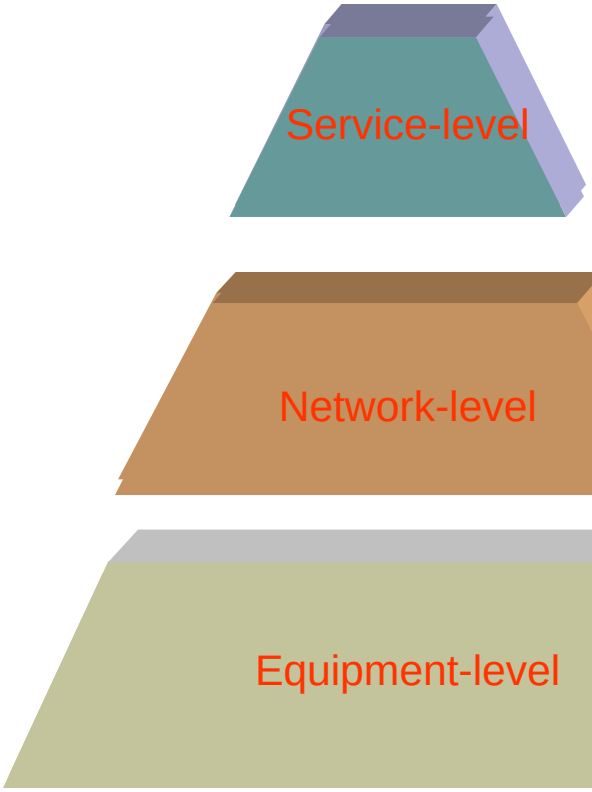


HUAWEI's research and practices – Find out configuration risk points on several levels



- **Analyze configuration correlations both on same level and different levels**
  - Consistency of configurations
  - Dependencies between configurations
  - Conflicts in configurations

HUAWEI's research and practices – Prevent misconfigurations on several levels



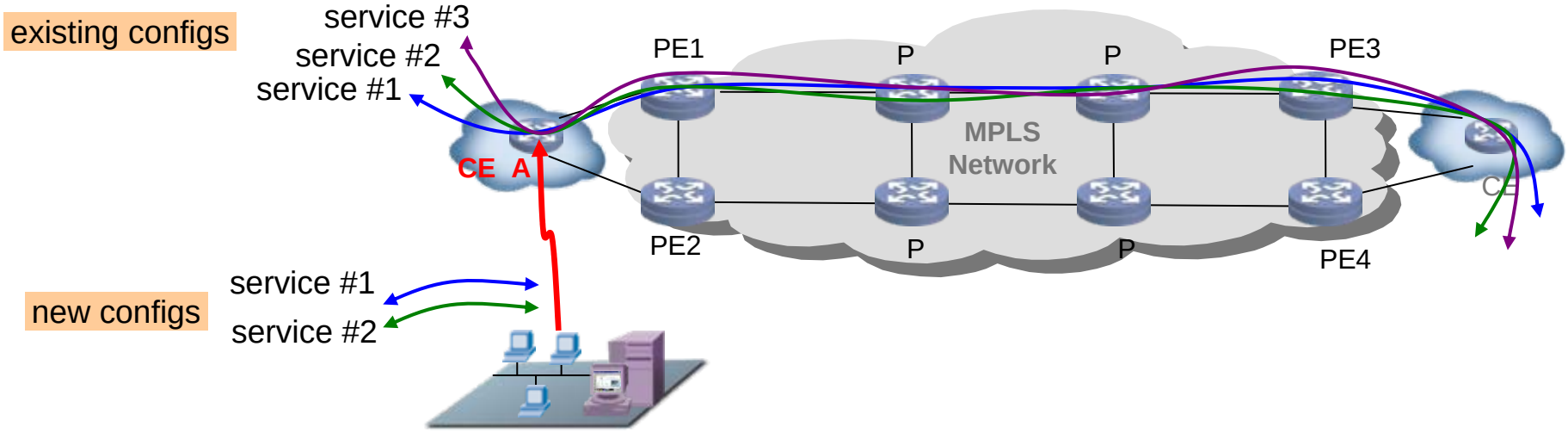
1. Configurations of different protocols, services and features: a service/function adapts itself to other services/functions automatically base on the configuration correlation analysis.

1.Deliver basic configurations of correlated NEs on the entire network automatically and in batches. Maintain consistency between different NEs.
2. Deploy consistent configurations on the whole network path to keep consistent between different NEs.

1. Template-based: User just need to input some data.
2. Wizard: step-by-step to finish complicated configurations.

HUAWEI's research and practices – An example

- **A familiar problem is to update a NE's configurations through a NM, an operation error can break the services**



- Service #3 will be lost on the whole network when the new configurations overwrite the existing ones and become active on equipment A.
- It's a misconfiguration risk point.
- **Check consistency** of the **existing configurations and new configurations** before allowing the new configurations to overwrite the existing ones.

Challenge and next step plans

- **Some actions for more complex future networks**
  - UCD project
  - Improve the methodology for complex-configurations analysis: focus on effective and rapid configurations-risk points discovery.
  - Network-level parameters correlation detection automation.
  - Tools to check and avoid misconfigurations when supplying system design.

Close co-operation between vendor and customer …