HITACHI
Inspire the Next

6QM Overview & Security Issues

David Diep

December 14th , 2004

6QM Workshop, Berlin

HITACHI
Inspire the Next

Contents

1 6QM Prototype Overview

2 Security Issues

3 Secured Deployment

HITACHI
Inspire the Next

Contents

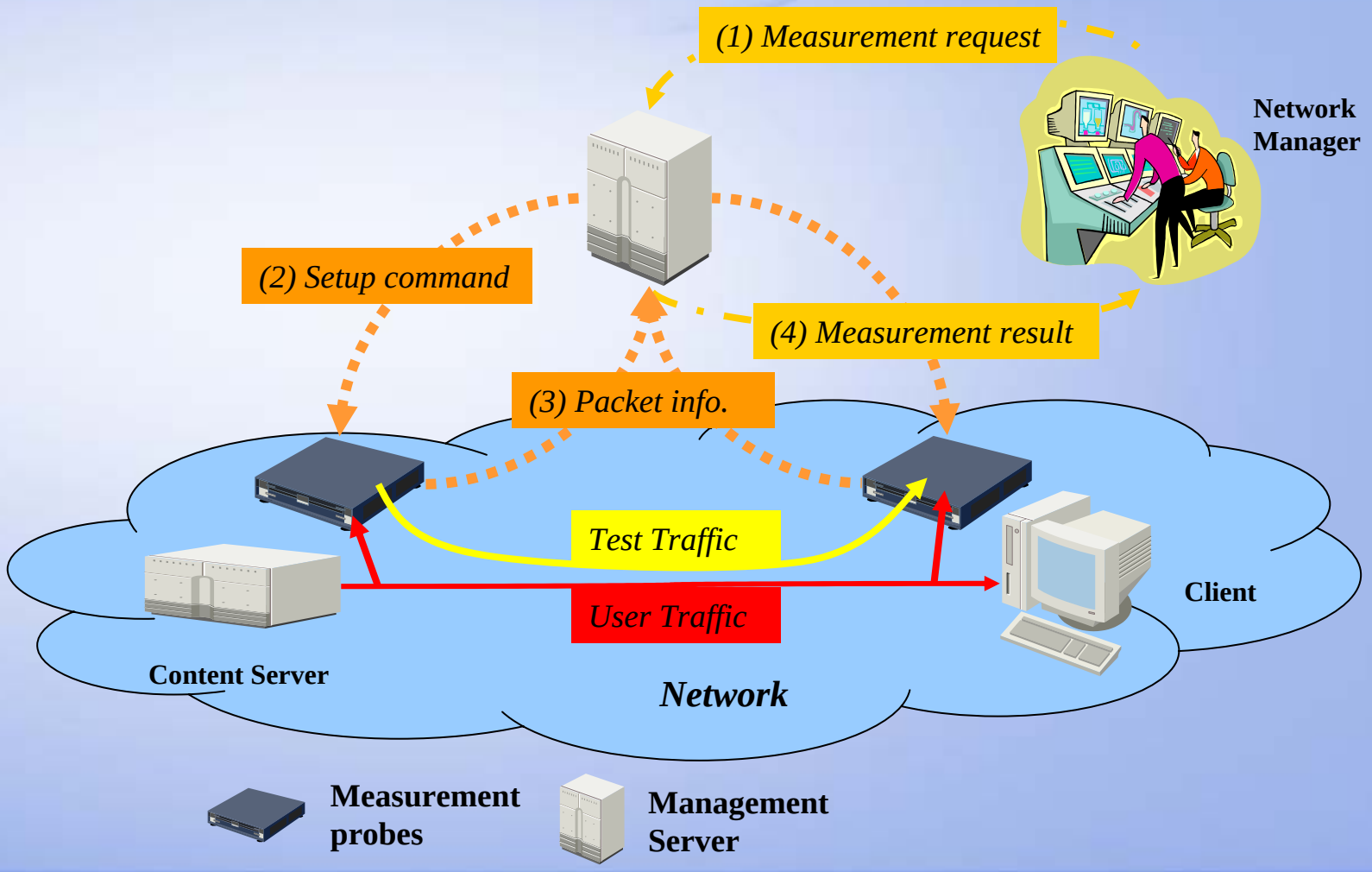
1 **6QM Prototype Overview**

2 Security Issues

3 Secured Deployment

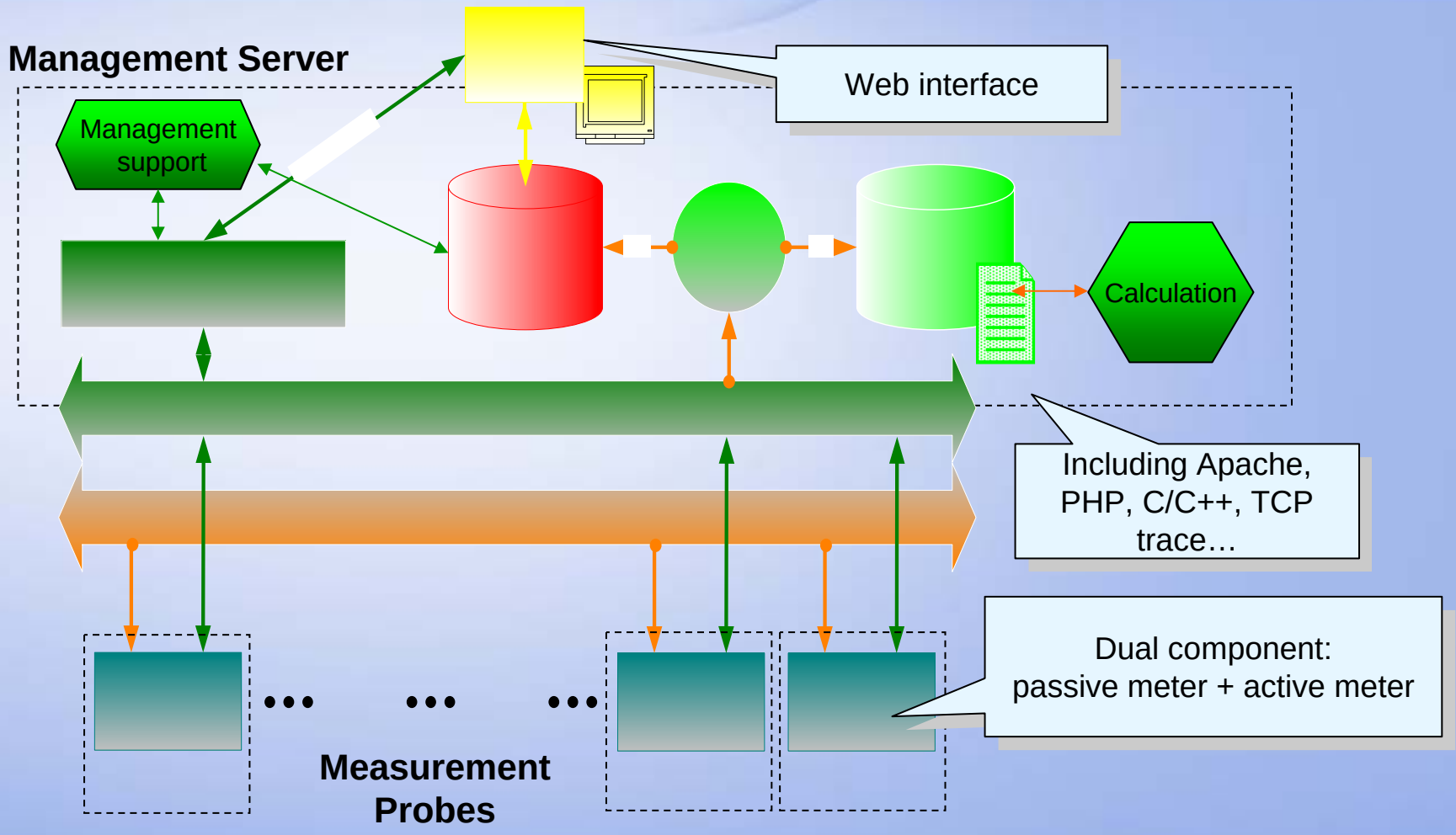
1 -1. Operation Overview

HITACHI
Inspire the Next



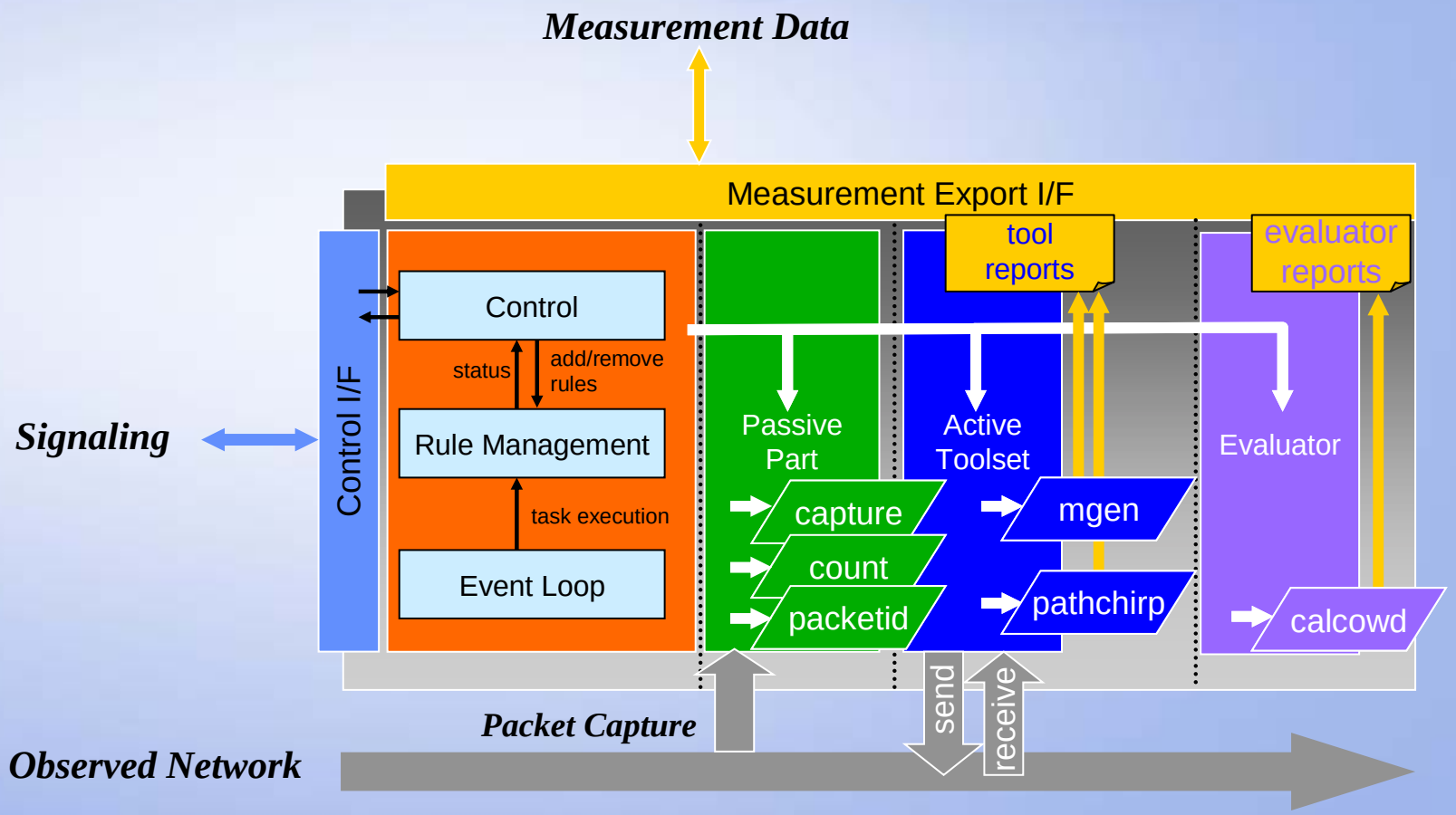
1 -2. Management Server

HITACHI
Inspire the Next



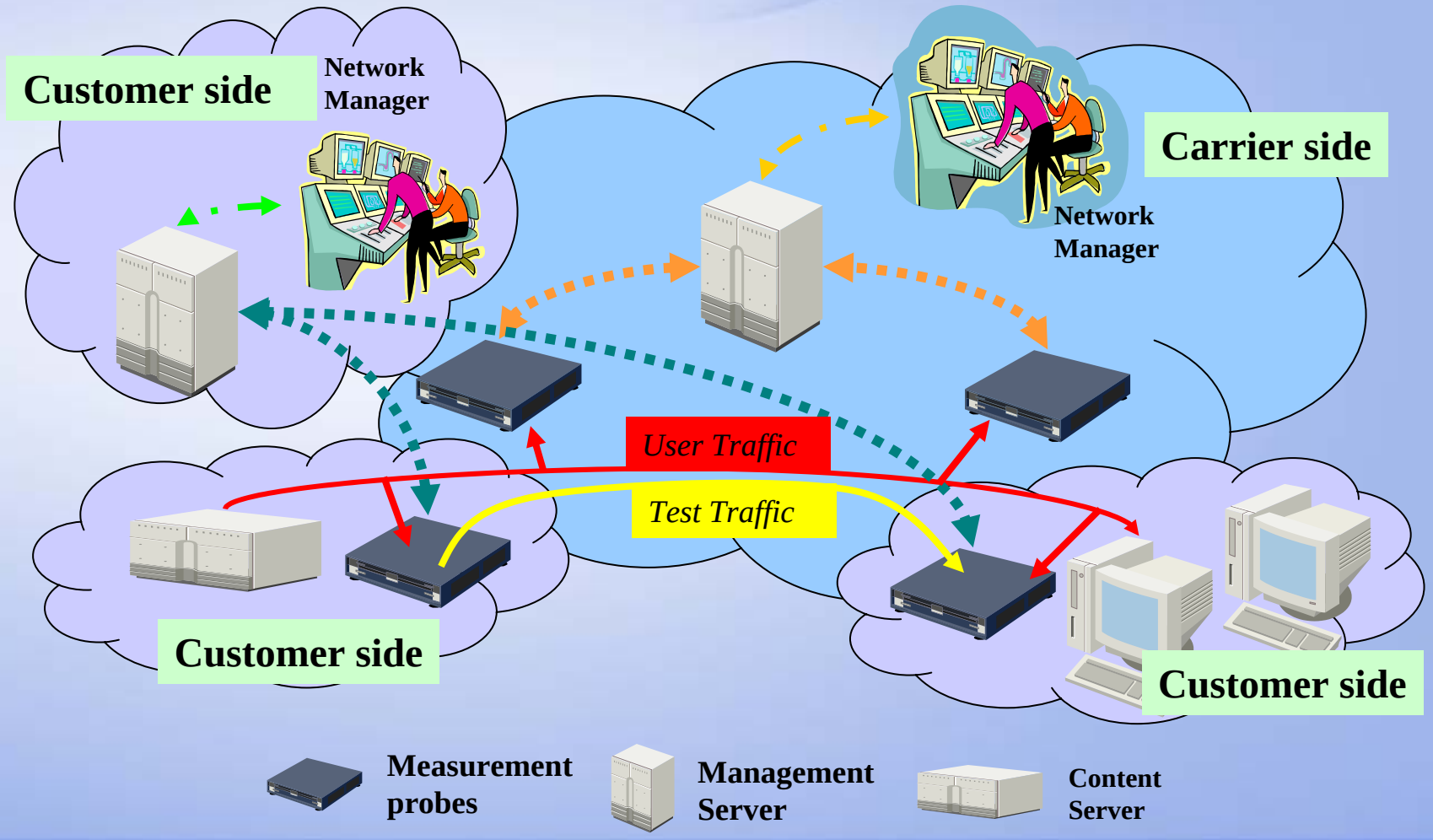
1 -3. Measurement Probe

HITACHI
Inspire the Next



1 -4. Deployment Scenario

HITACHI
Inspire the Next



HITACHI
Inspire the Next

Contents

1 6QM Prototype Overview

2 **Security Issues**

3 Secured Deployment

2 -1. Security Objectives & Risks

HITACHI
Inspire the Next

- Protect measurement data
  - Keep confidentiality of the measurement result
    - Ensure confidentiality of user information when user packet is captured
    - Ensure non disclosure of performance information (e.g. ISP policy)
  - Keep integrity and authenticity against malicious modifications
    - Operational risk if unjustified alarm is triggered (network management aspect)
    - Financial risk if connection with billing (e.g. SLA based carrier business model)
- Avoid illicit usage of the measurement system
  - Avoid the system to become an infrastructure for eavesdropping (monitoring allows packet capture)
  - Avoid outsiders to use the system
  - Avoid system users to do anything on the system
- Avoid to have an open door for other attacks
  - Avoid measurement host server to be pirated and controlled by malicious persons

2 -2. Environment

HITACHI
Inspire the Next

- Environment increasingly dangerous
  - Generally the attacks and virus are increasing
- In our case specifically
  - Not always a separate network for the management
    - Need to secure the communication between measurement components
    - Need to secure the communications between operator and management server
    - Need to protect the measurement hosts
  - Even in secured environment different levels of access are still required
    - Need to restrict user access based on authentication
    - Need to restrict system user right based on credential
  - Future Inter-domain measurements
    - Need to build a trusted environment among the partners
    - Need to secure information exchange

HITACHI
Inspire the Next

Contents

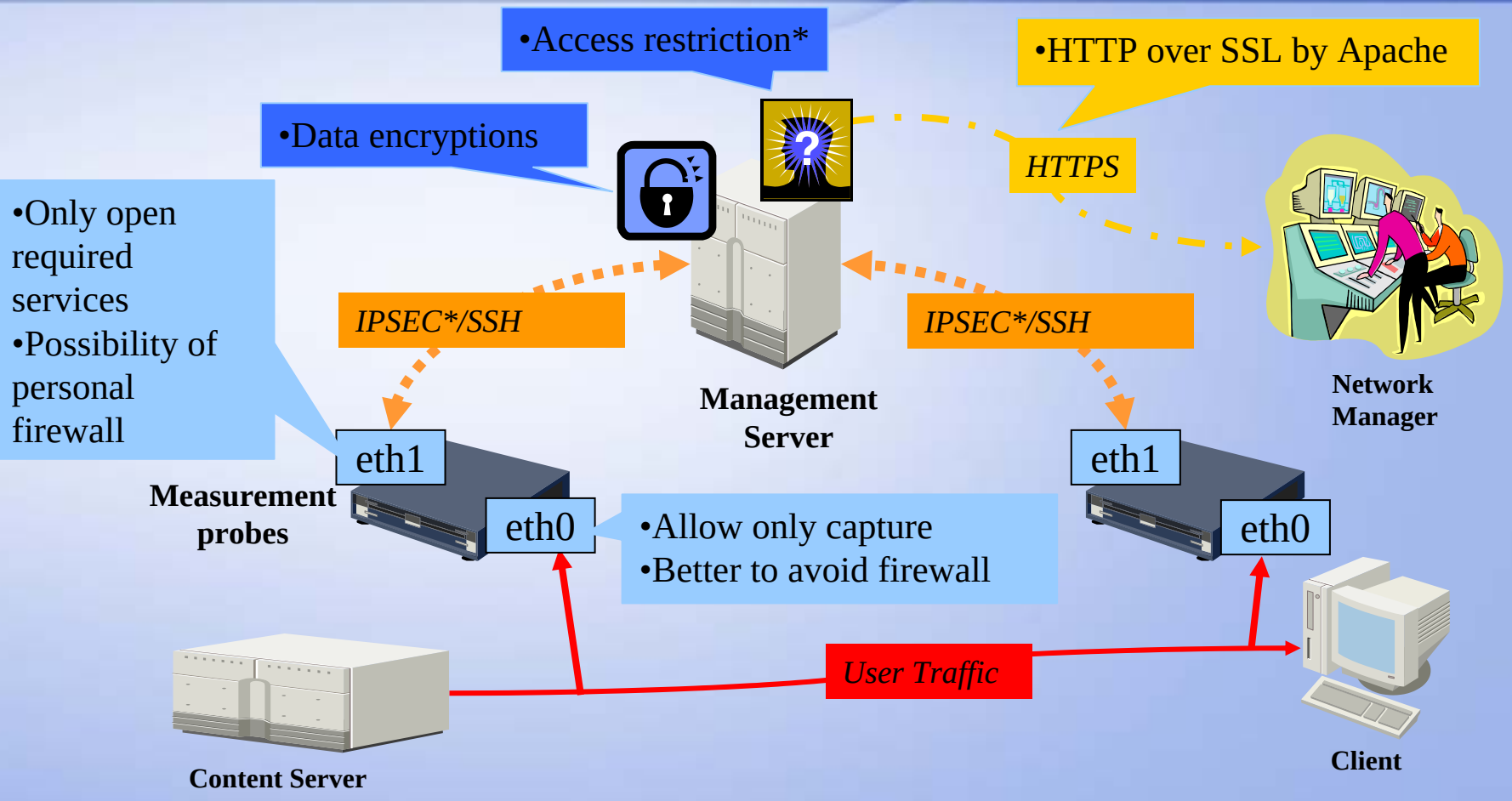
1 6QM Prototype Overview

2 Security Issues

3 **Secured Deployment**

3 -1. Secured Deployment

HITACHI
Inspire the Next



* More details provided later

3 -2. IPsec (1/2)

HITACHI
Inspire the Next

	Advantages	Drawbacks
IPsec	- Support any transport protocol (appropriate for IPFIX extension with UDP/SCTP) - Usage managed independently from the prototype code - Should become highly available in the future as mandated in IPv6	- Currently not always available on production hosts (may require kernel recompilation) - May have interoperability issue - May interfere with NAT and firewall
SSH	- Highly available (usually enable on existing hosts) - Application granularity	- Specialized in TCP services (problematic for IPFIX extension with UDP/SCTP)

- IPsec is appropriate to secure various protocol over IP
- If specific equipment is shipped by vendors, availability of IPsec is not an issue

3 -3. IPsec (2/2)

HITACHI
Inspire the Next

- Various configurations exist in IPsec (must be agreed between peers)
- If possible keep light configuration to save host resource
- Suggested settings
  - Enable ESP for encryption, integrity and anti-replay (e.g. 3des-cbc)
  - Enable Authentication
    - ESP (e.g. hmac-md5 or hmac-sha)
    - Or AH (e.g. hmac-md5 or hmac-sha)
  - Mode: transport
    - Not much benefit for tunnel as it is point-to-point communications
  - Automated key exchange
    - Better avoid manual keying (no anti-replay protection)
    - IKE:
      - public/private key scheme (RSA)
      - Avoid shared secrets for scalability issue
- Availability: Free implementation
  - USAGI for Linux based on Free/SWAN implementation
  - KAME for BSD

3 -4. Access Restriction

HITACHI
Inspire the Next

- Simple Access Restriction to system functions
  - Relying on Apache to block access to some management pages
  - Not always enough (depending on scenario)
- Advanced Access Restriction
  - Concept (introduced in revised specification)
    - Definition of user roles (such as user manager, system user)
    - Define access to meter and task execution rights on user granularity
  - Not implemented in the prototype

	Functions		
Role	**Management / Assignment User Privileges**	**Management System Components**	**Management Measurement Tasks**
System Administrator		X	
User Manager	X		
System User			Explicit Permissions

Conclusion

- Importance of security
  - Keep confidentiality of user data
  - Make people feel secure about using QoS monitoring is a key point for success
- Security is tightly related to the system deployment and configuration
  - Relying on external elements and configuration
  - Relying on each network policy

HITACHI
Inspire the Next

THANK YOU!