NMRC

Promising Network Management Research Areas: A Network Vendor's Perspective

Petre Dini, Cisco, USA
pdini@cisco.com

© 2006 Cisco

Network Management Research Council

- The NMRC is a task force within Cisco, organized out of the CTO Office of Cisco's Network Management Technology Group.
- Mission: Facilitate interaction between Cisco network management product development groups and researchers who investigate areas of potential interest to those groups.
- Cisco support may include funding of joint research projects
  - Cisco's University Research Program (URP)
  - Cisco Applied Research and Development (CARD) projects.
- Goal for this workshop: Present an overview of some research areas that promise to have substantial practical relevance and commercial impact by addressing existing and future network management needs of Cisco customers.

© 2006 Cisco

Application Service Assurance

- **Business Drivers:**

  Service Providers want to become Experience Providers

  Enterprise IT needs to rapidly deliver new business applications to distributed, fluid organizations

- **Technical Enablers:**

  Advances in measurement technologies enable the detection, monitoring and control of individual application flows as they traverse the network

- **Some related research areas**

  Resource to *app-flow* to *user QoE* performance correlation

    service path (app-flow to resource)

    user QoE to app-flow

  Network performance data mediation

  Performance policy optimization

  User QoE definition and measurement

© 2006 Cisco

Autonomous Networks

- **Business Drivers:**
  - Service Providers and Enterprise IT want to reduce management costs
  - Service Providers and Enterprise IT deal with complex management systems, advanced services, multi-facet customers
- **Technical Enablers:**
  - New paradigms on system automation, prediction, formalized intuitions
  - New approached for defining and processing trust, incomplete and temporal data
- **Some related research areas**
  - Adaptable entities
  - Self-management
  - UP&P
  - Ambient Networks
  - Design methodology for autonomic entities
  - Self-ilities

© 2006 Cisco

Models for systems and their management

- **Business Drivers:**

  Network, service and technology convergence

  Service Providers and Enterprises deal with complex management systems, advanced services

- **Technical Enablers:**

  ITU Recommendations, DMTF, TMF, OASIS, 3GPP

  Existing focus groups NGN, NGN Mgmt, TISPAN, ….

- **Some related research areas**

  Federated models

  Reflexive models for dynamic behavior

  Context-based model translators

  System modeling languages

© 2006 Cisco

Policy-enabled managed and management systems

- **Business Drivers:**
  - Experience reuse for reduced management costs of complex systems
  - Enterprise IT and Service Providers need to dynamically adapt to evolving systems, dynamic situations and changing user profiles
- **Technical Enablers:**
  - Policy languages cover (partially) the needs
  - Commercial (simple) policy engines exist
- **Some related research areas**
  - Policy translations (goals…executable policies)
  - Dynamic policies
  - Distributed policies
  - Policy conflict detection/resolution
  - Enhanced, yet user friendly, policy languages

© 2006 Cisco

Additional topics to be considered

- Web services for management
- IPv4/IPv6
- P2P traffic models
- Forensic/(near)real time/proactive/ diagnosis
- Overlay networks
- Service lifecycle (composition)
- Delay tolerant networks
- Context-based correlation
- Embedded instrumentation (e.g., service oriented)

© 2006 Cisco

© 2006 Cisco

Back-up for discussions

© 2006 Cisco

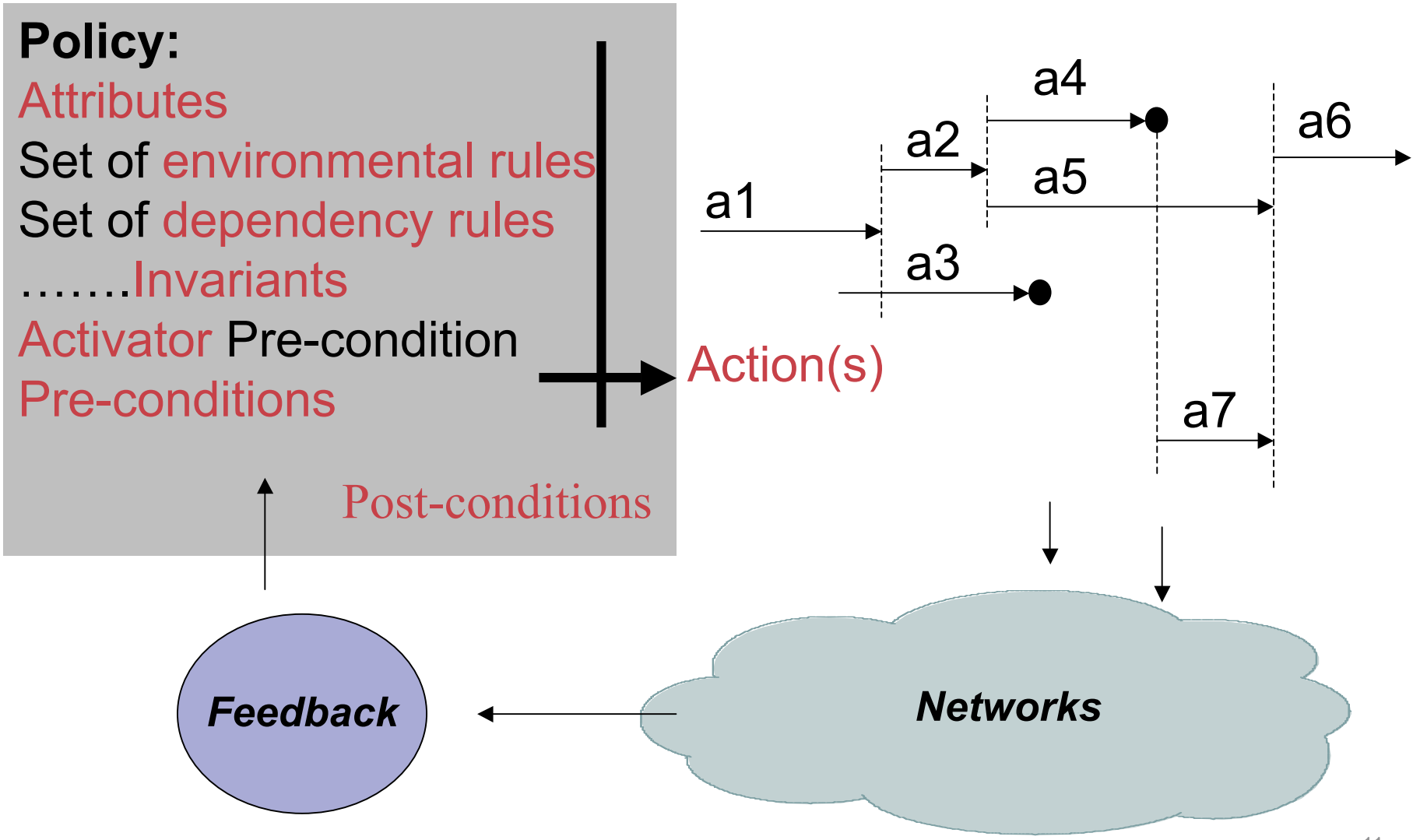
Detailed cases

- Policy-enabled
- Autonomic Networks
- Application Service Assurance

© 2006 Cisco

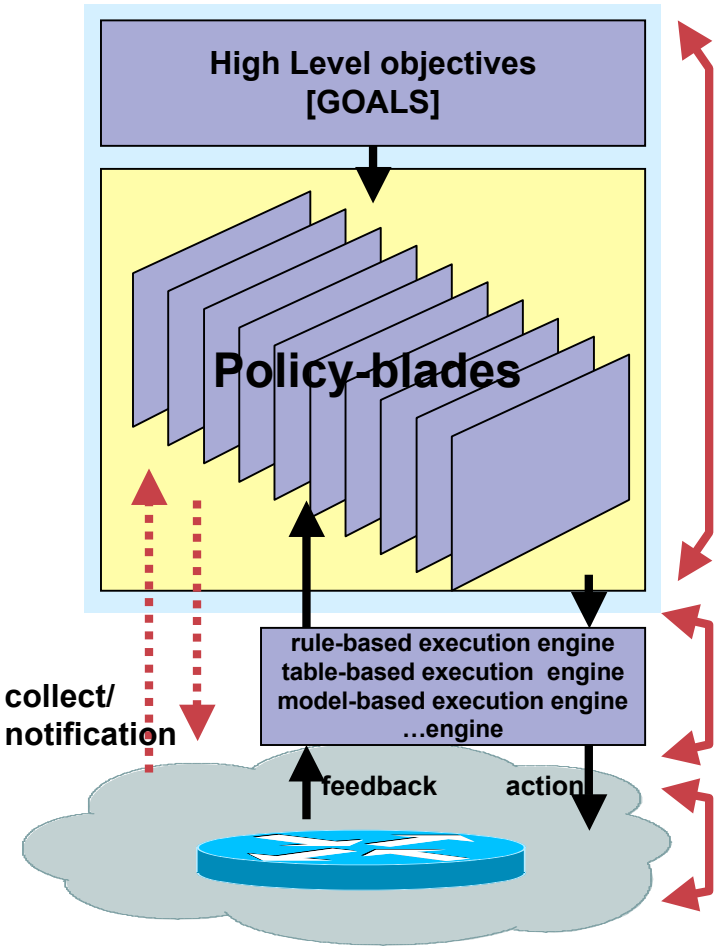
What is a policy?

High level policies → low level policies



© 2006 Cisco

Goals→Policy→ Actions translation



- Fuzzy middle between a human desire and a machine definition:
- Goal: *I want to encrypt and authenticate <all access> that my <subcontractors> have to <my network>*

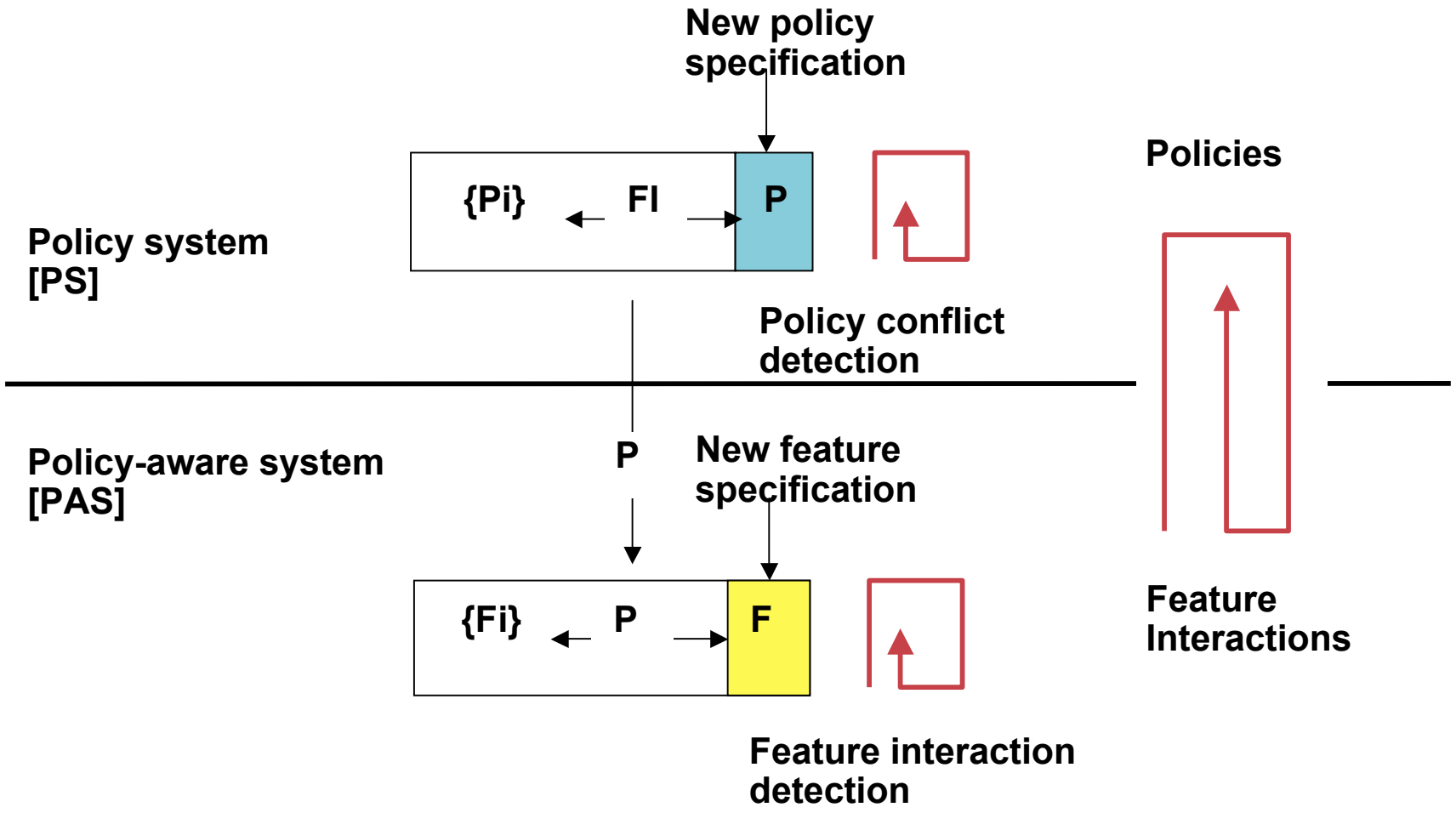
Translate: *<from:> <to:> and <keep_link:goals-policies>*

Policy Definition: Authorize <owner/system> to *Encrypt <TCP packets> from <10.3.86.5> to <10.4/16> with <CAST> and Authenticate them with <HMAC-SHA>*

Policy Execution:
Authorize <owner/system> to
(rules to authorize…)
Encrypt <TCP packets> from
(selection, encryption, etc.)
<10.3.86.5> to <10.4/16> with <CAST> and
Authenticate them with <HMAC-SHA>
(authentication methods…)

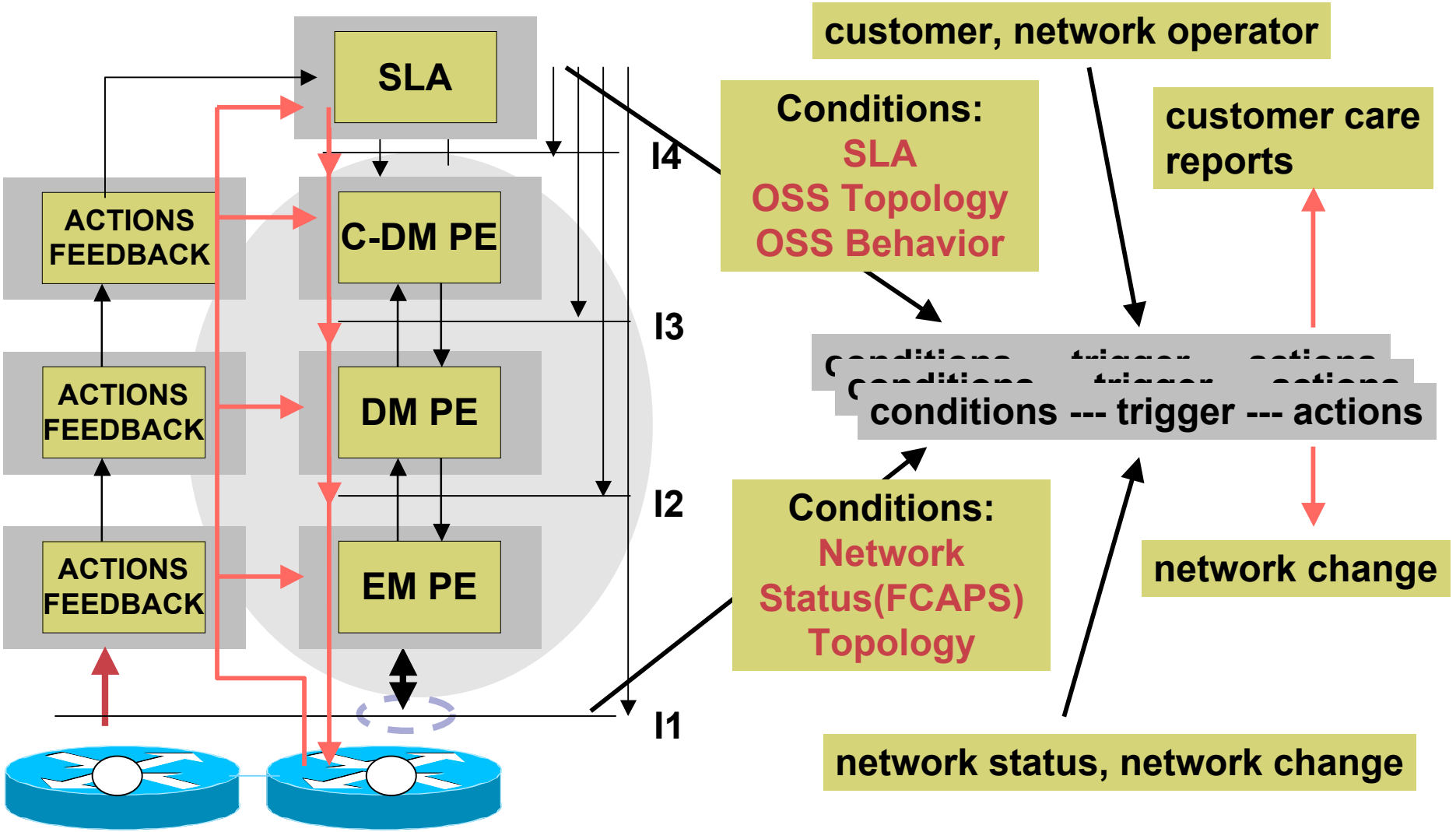
© 2006 Cisco

Policy interactions for added value services



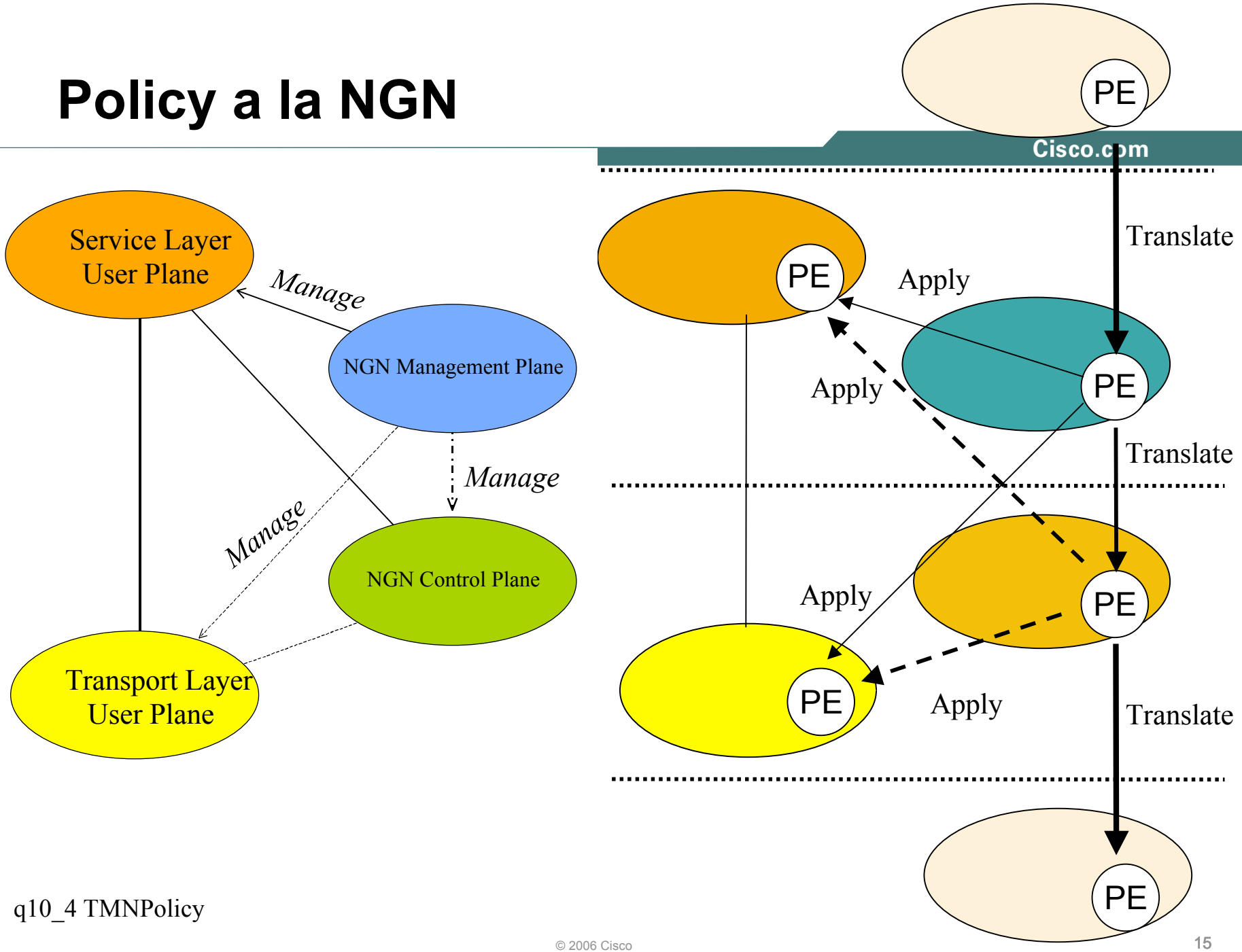
© 2006 Cisco

Policy distribution



© 2006 Cisco

Policy a la NGN



© 2006 Cisco

Smart Call Home vs. Overall Self Management

- Self Management can be defined as the ability for network administrator or end user to simply plug in the device, powers it on, and then the device
  - Upon plug in, device connects itself to the network
  - Device configures itself
  - Device starts communicating with other devices and networks
  - Device Self manage itself: Smart calls home for alarms, latest config updates, etc.
- Which devices should be self managed?
  - Core devices
  - Distribution Network
  - Access Network
  - Subscriber Network/Customer promise

© 2006 Cisco

Smart Call Home (SCH) Overview

- **What is Smart Call Home?**
  - – Allows devices to provide real-time alarms, proactive notifications, and inventory updates to backend systems and TAC
- **Why Smart Call Home?**
  - – Provider is alerted of customer problems/potential problems BEFORE customers
  - – Expedite resolution and recovery: TAC starts working on critical alarms immediately
  - – Increase RMA and decrease number of SRs entered by customers
  - –Latest bug related data
- **What is required for Smart Call Home?**
  - – Access and collection of detailed inventory and diagnostic data to solve problem quickly (No need to keep call customers/keep them on line, or asking them to run cases to obtain the required data). Periodic data collection vs. sending specific inventory data as part of SCH messages
  - – Algorithms for alarms collections and filtering: SCH is not a fault management systems. Only very specific alarms should be sent to TAC. Other alarms may need to be logged. How to determine which alarms to send to TAC vs. fault management system alarms vs. logged alarms?
  - – Rule processing capabilities to inform customers of resolution steps
  - – Notification algorithms: Who to notify (end users/subscribers, network admins, management partners, other Cisco organization) and by when?
  - – Standard protocols for SCH (e.g XML, Web Services) so multiple vendors networks.
  - –Methods and procedures to capture install based knowledge (inventory, configuration, software images) for sale teams.

© 2006 Cisco

Challenges

- Standards (for services, APIs, management protocols, etc.)
  - Too slow to define and adapt (e.g. DSL)
  - Too many standards
- Services are getting to complicated (IPTV, IP Video conferencing)
- Short life cycles for services and technology
- Huge and expense existing systems and methods of operation
- Difficult to obtain:
  - Accurate view of network inventory
  - Accurate view of software images
- Accurate service contract for service providers (i.e. UDI, Serial Number, Product ID)
- Network Security: many SPs are not willing to share inventory data
- Subscriber Security: many SPs are concerned about security of their customers data.

© 2006 Cisco