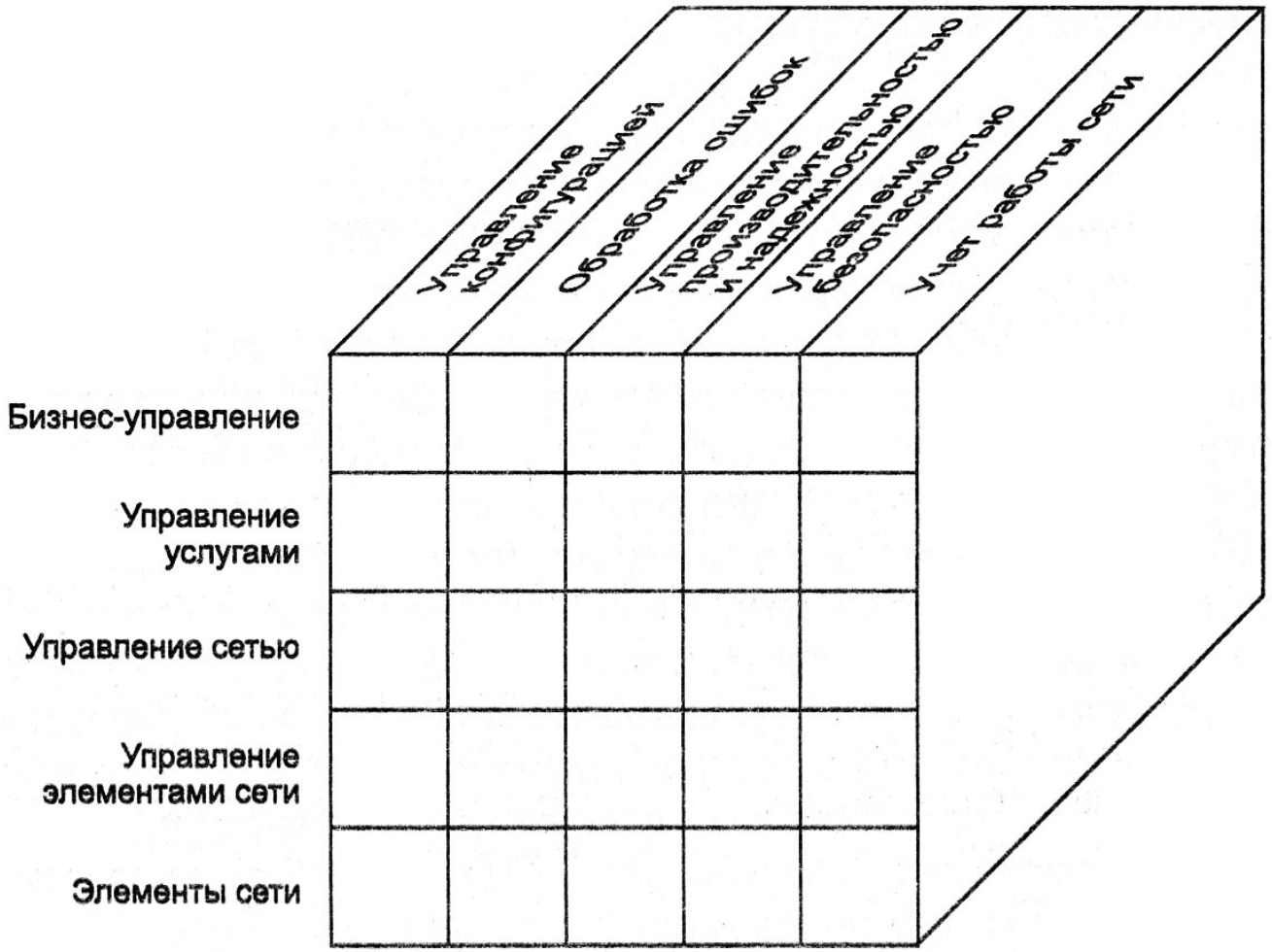
Управление сетями, функции

- В стандартах ISO7498-4, ITU-T X.700, связанных с управлением сетями, выделяют пять функций управления:
- Управление конфигурацией (configuration management)
  - Изменение параметров объектов управления и управление их связностью, конфигурирование
- Обработка ошибок (fault management)
  - Оповещение об ошибках, ликвидация аварийных ситуаций
- Анализ производительности (performance management)
  - Сбор статистики с объектов управления, определение узких мест
- Управление безопасностью (security management)
  - Включает в себя управление механизмами обеспечения целостности, конфиденциальности и доступности информации в системе
- Учет работы (accounting management)
  - учет использования ресурсов сети

Применительно к компьютерам и ПО (System Management system)

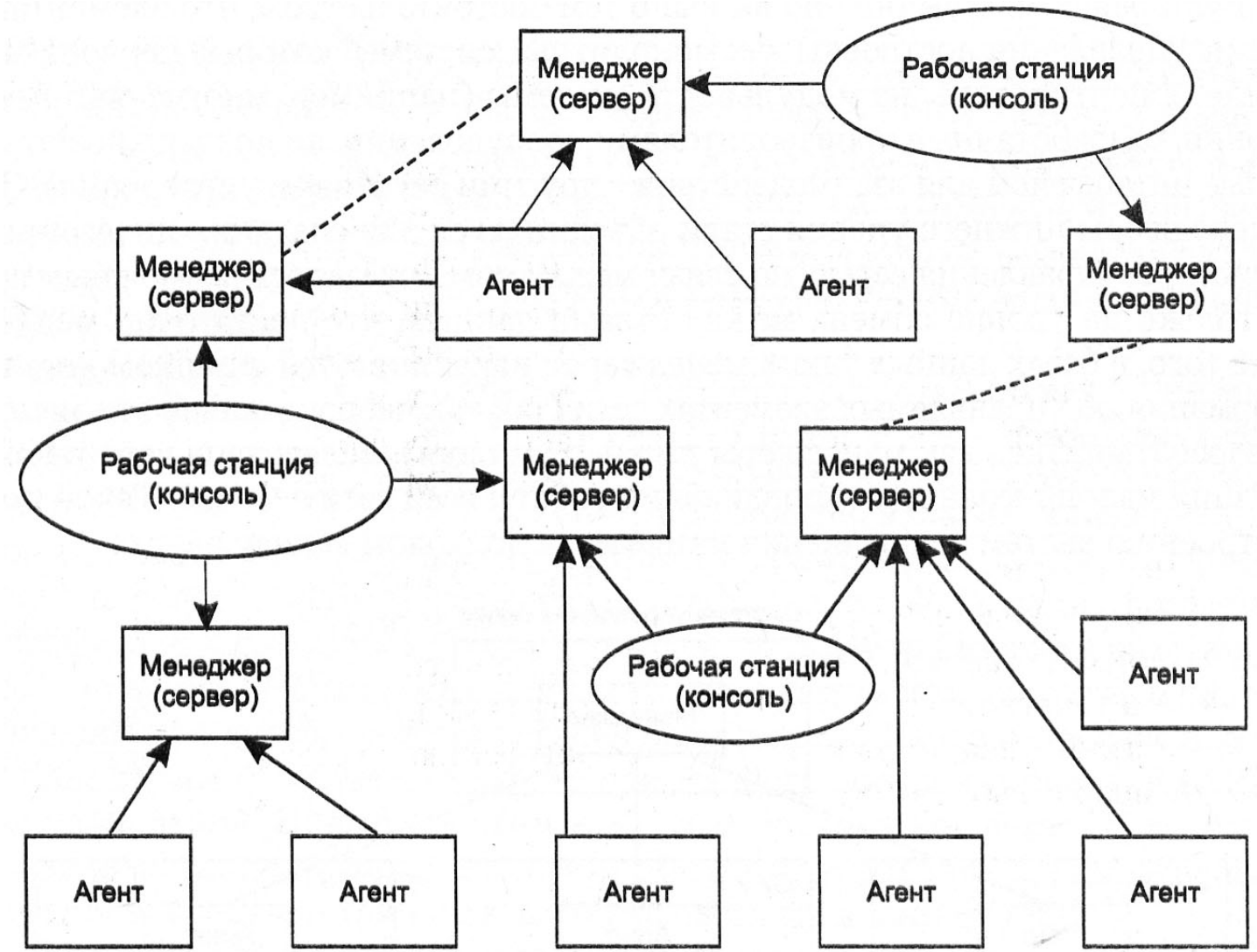
- Стандартные функции SMS
  - Учет аппаратных средств и ПО
  - Установка ПО
  - Контроль производительности и ошибок
- Примеры SMS: MS/SMS, IBM/Tivoli, Norton/Ghost (частично)

Многоуровневое представление задач управления сетью



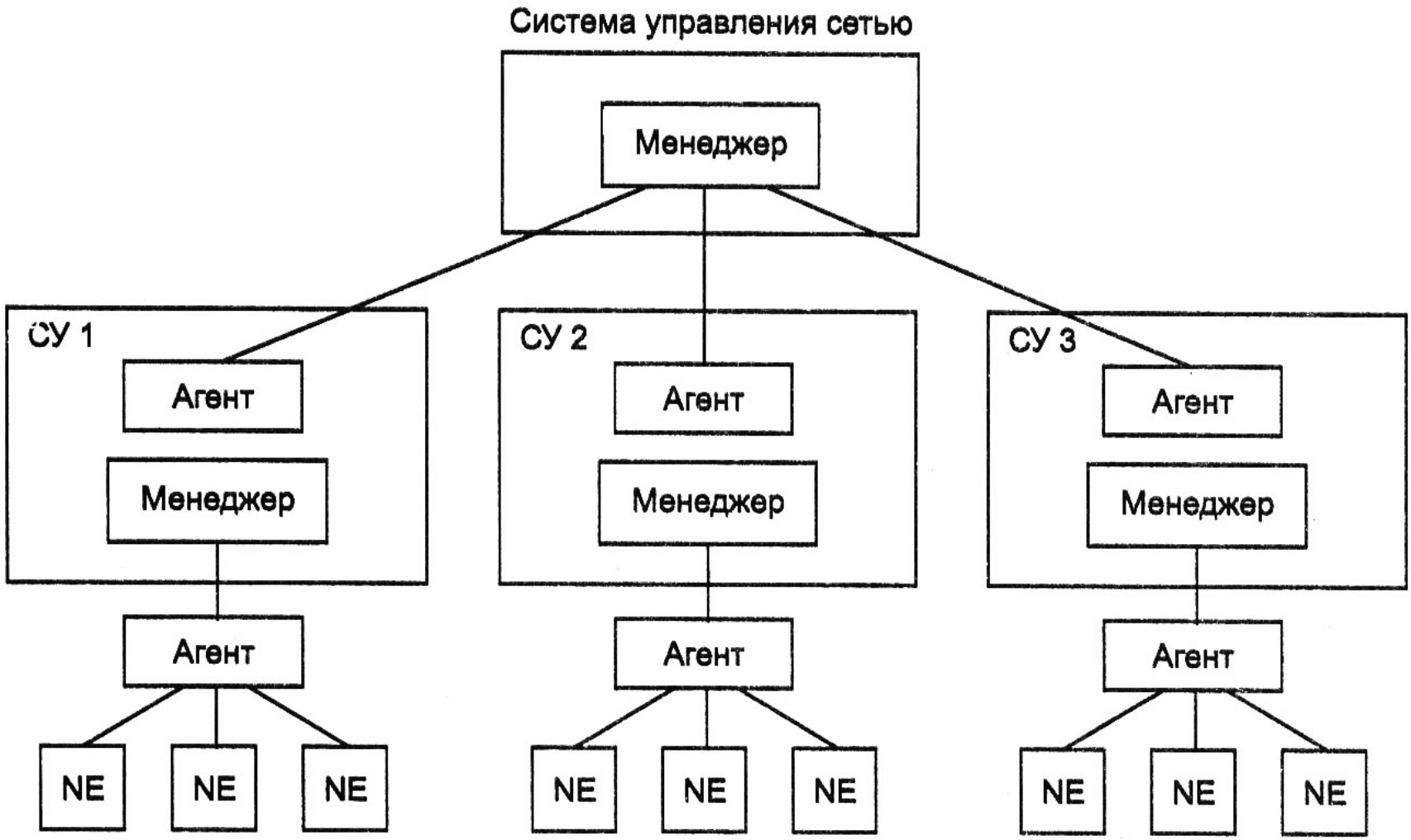
Взаимодействие агента, менеджера и управляемого ресурса

Распределенная система управления

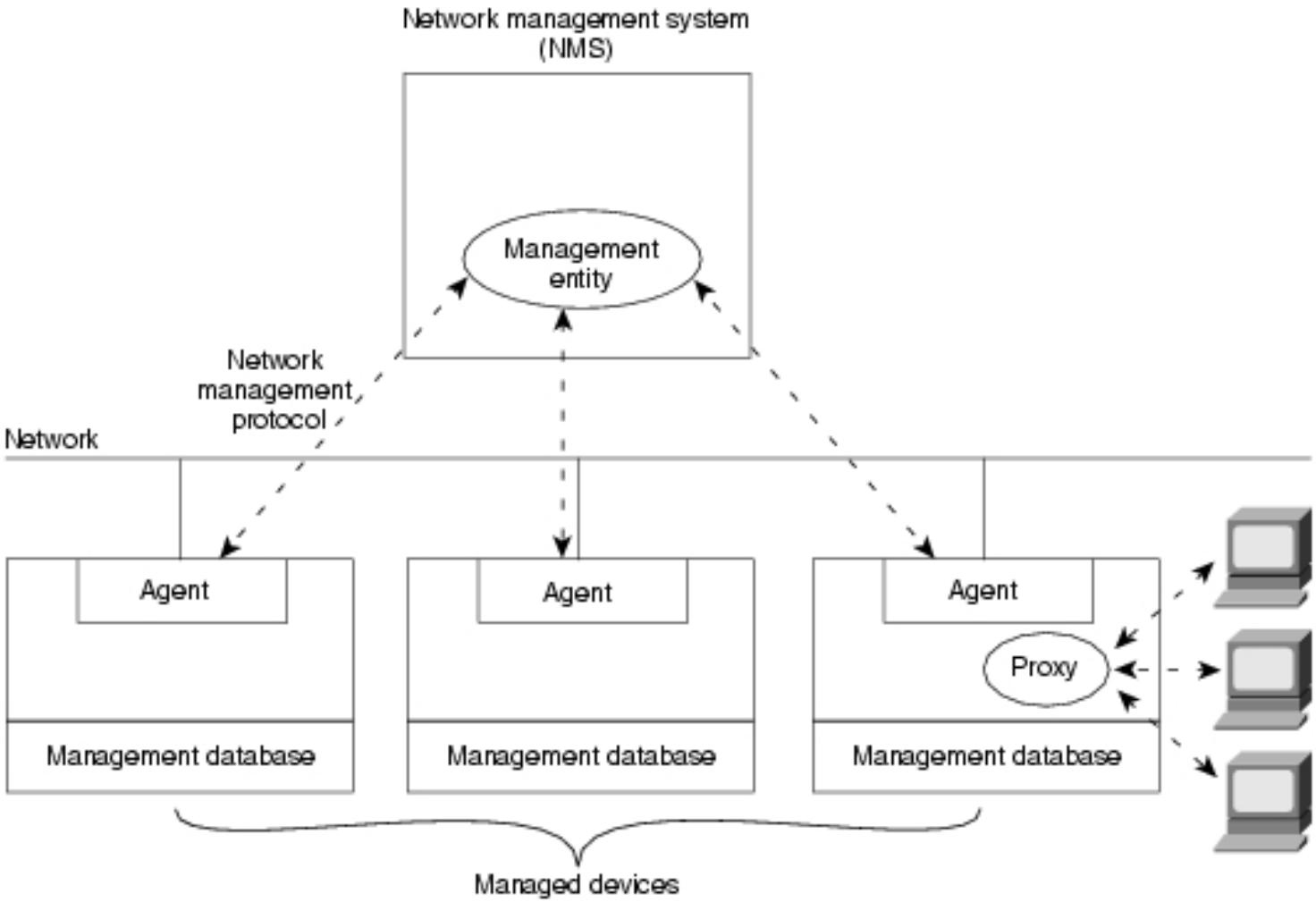


Одноранговые связи между менеджерами

Иерархические связи между менеджерами



Типичная архитектура управления сетью. Использование прокси.



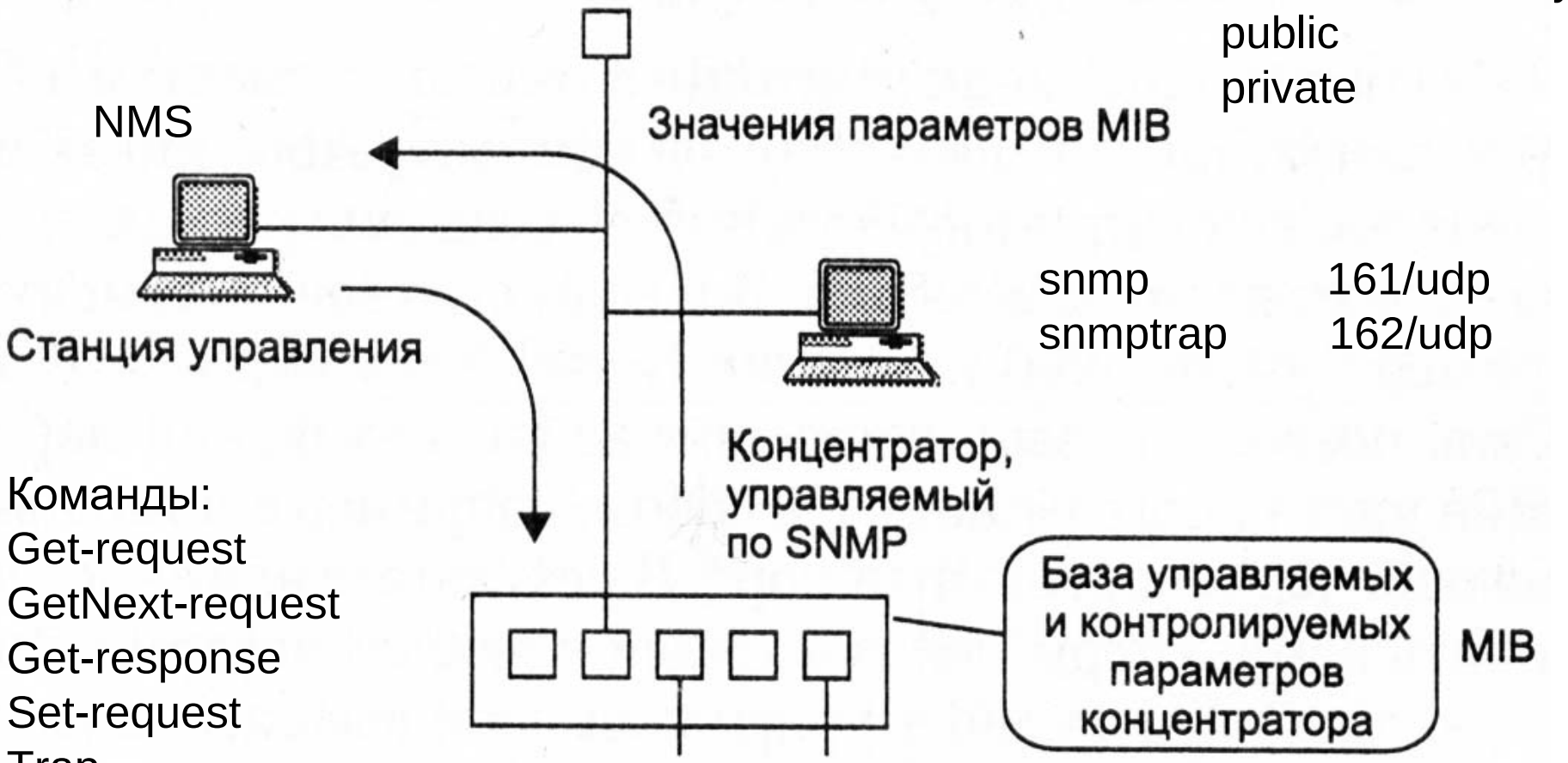
Типы управления по степени автономности

- in-band management – управление сетевым оборудованием «через сеть». Примеры: SNMP, Telnet, SSH.
- out-of-band management (иногда Lights-out Management, LOM) - управления извне сети, через выделенные каналы обслуживания. Примеры: последовательные консольные порты, dial-up модем, использование независимых систем электроснабжения. Работает независимо включено/исправно ли сетевое и серверное оборудование.

Управление сетями, интерфейс менеджер-агент

- SNMP (internet, разработан университетом Тенесси (США),1988г.)
- Common Management Information Protocol, CMIP (ISO/OSI)
- Описание форматов протоколов, переменных MIB использует формальный язык ANS.1, принятый в ISO как стандартная нотация для коммуникационных протоколов
- Реализации SNMP: Carnegie-Mellon University CMU-SNMP; University of California, Davis UCD-SNMP; SourceForge Net-SNMP

Система управления на основе SNMP

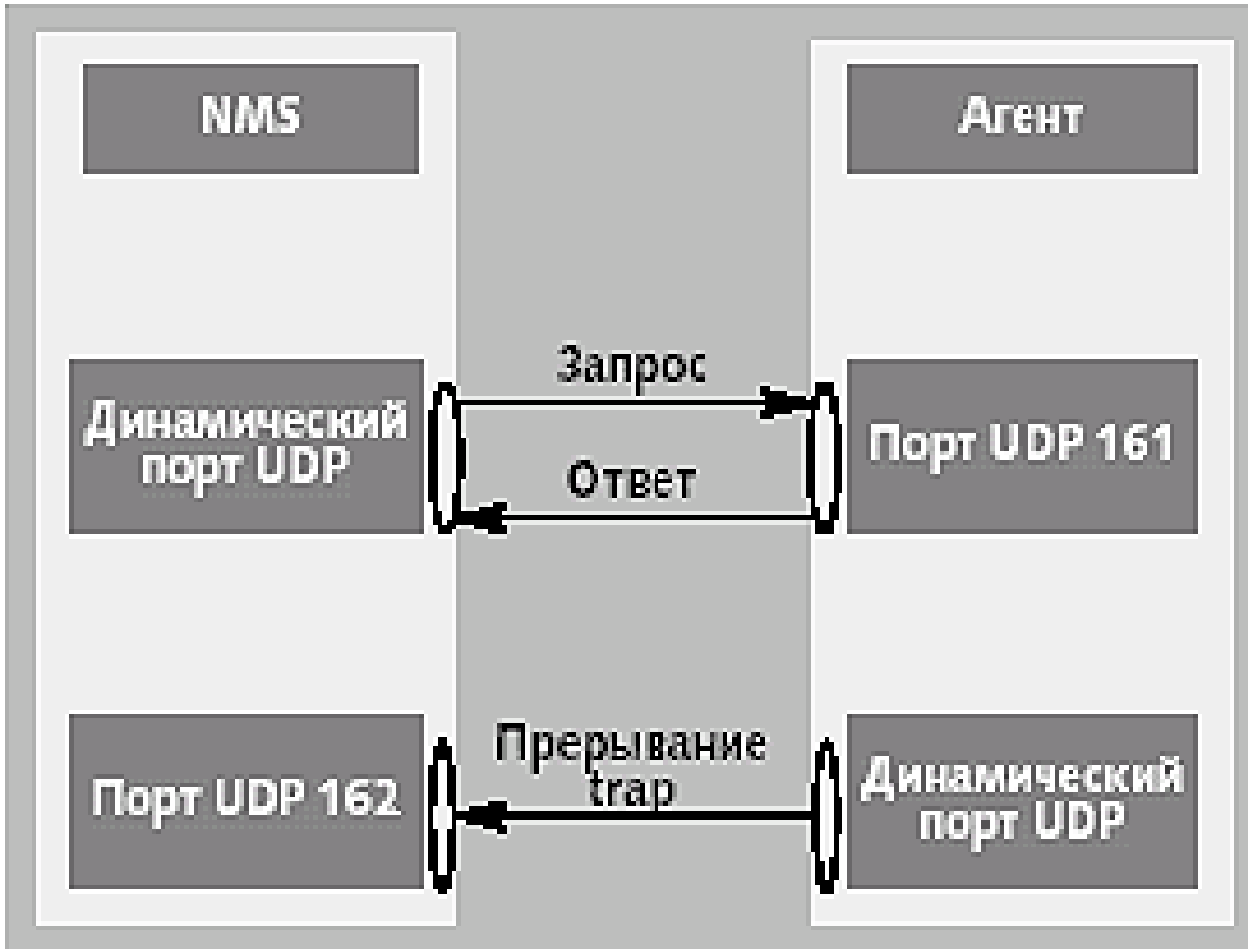


Безопасность: community
public
private

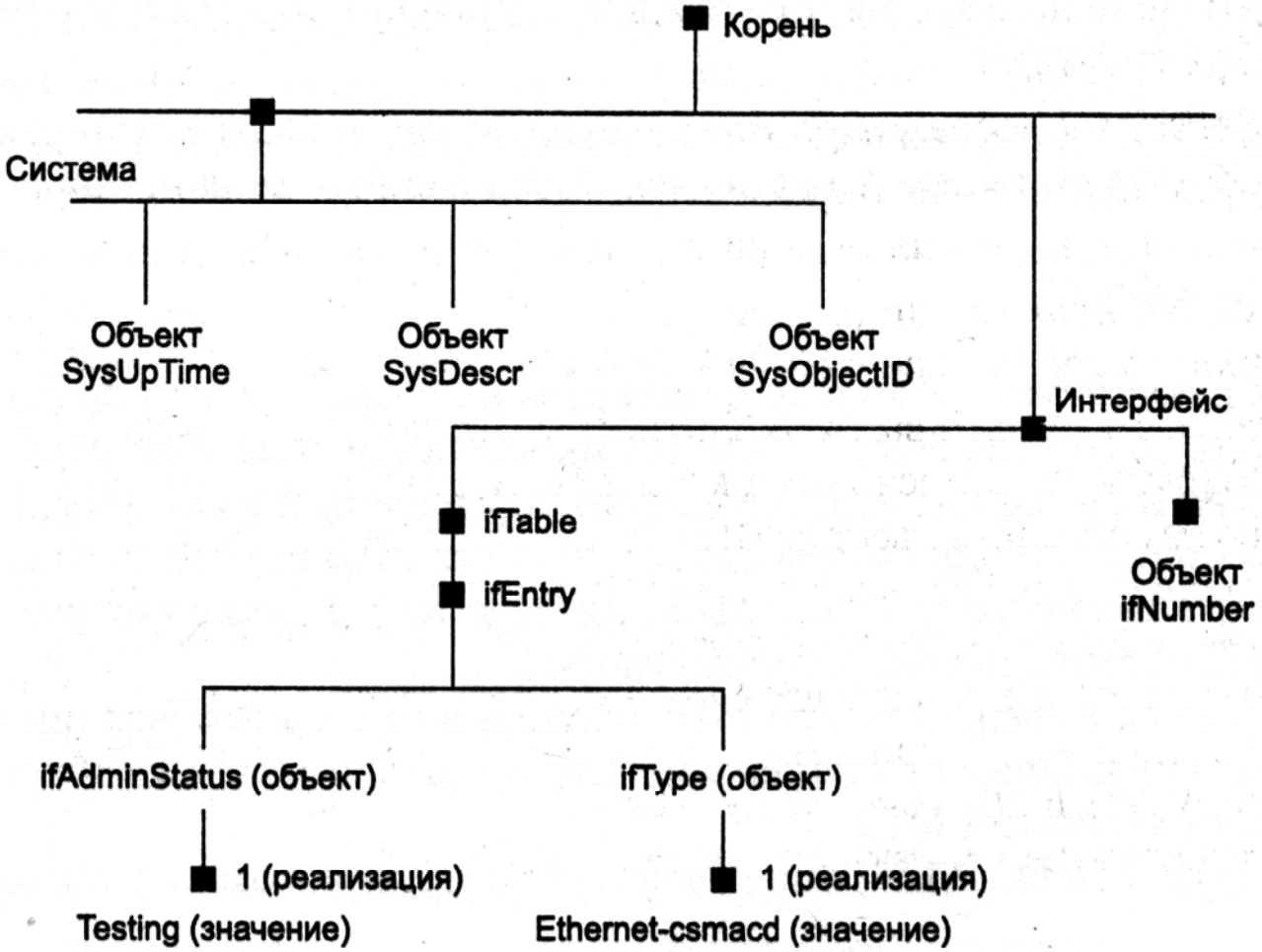
snmp 161/udp
snmptrap 162/udp

Команды:
Get-request
GetNext-request
Get-response
Set-request
Trap
GetBulk

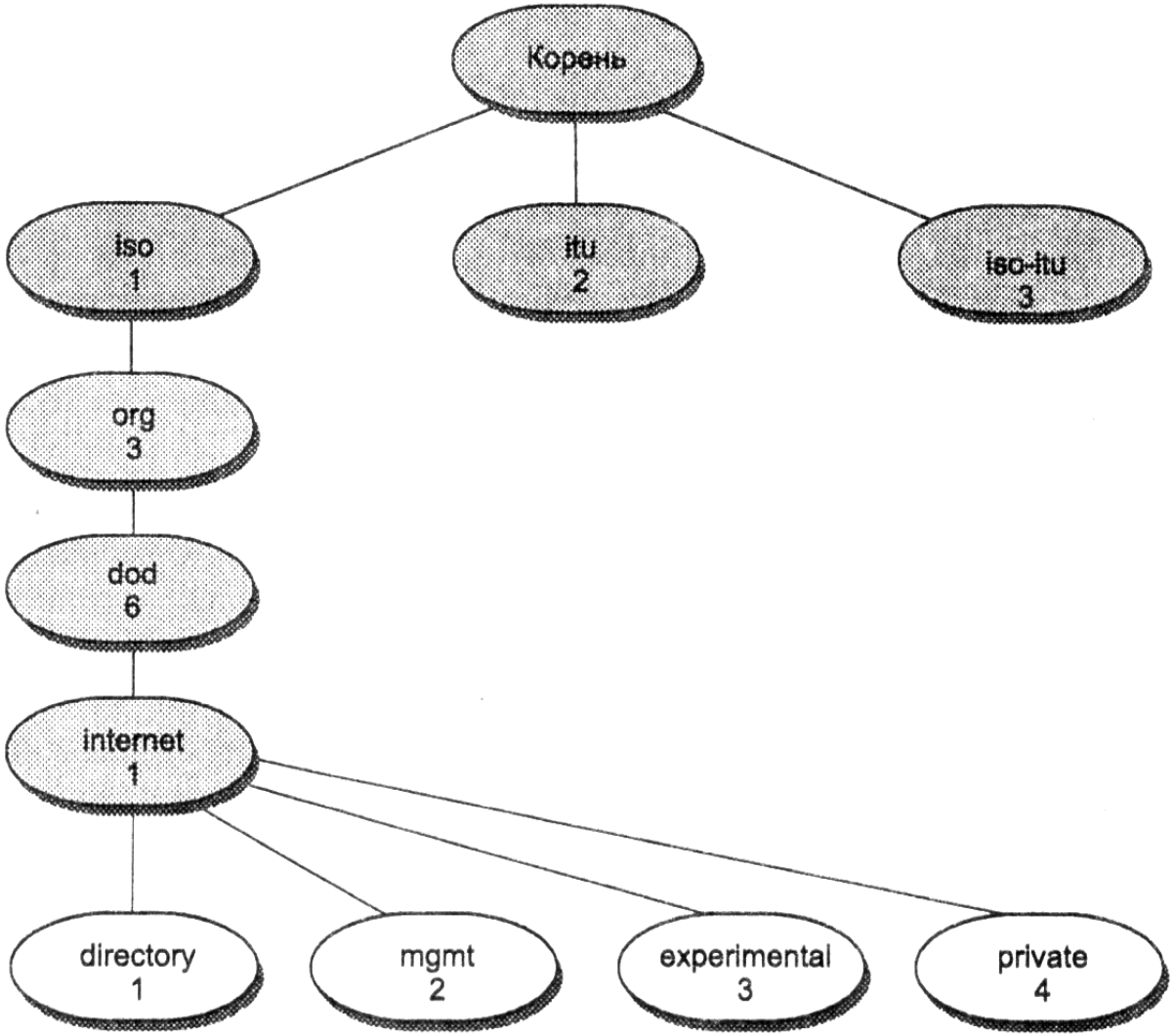
Работа SNMP через UDP



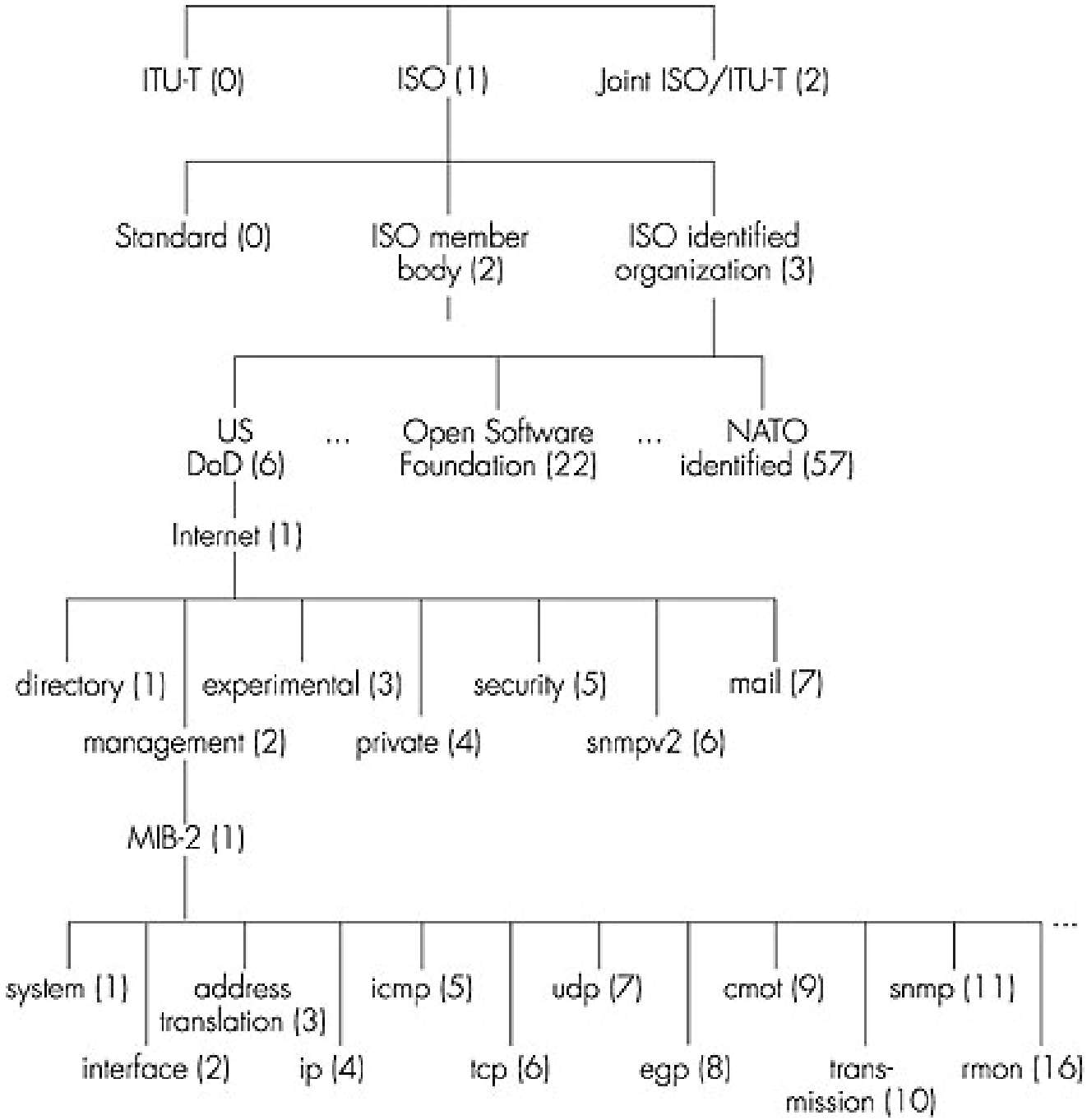
Структура базы SNMP MIB



SNMP MIB (пространство имен объектов ISO)



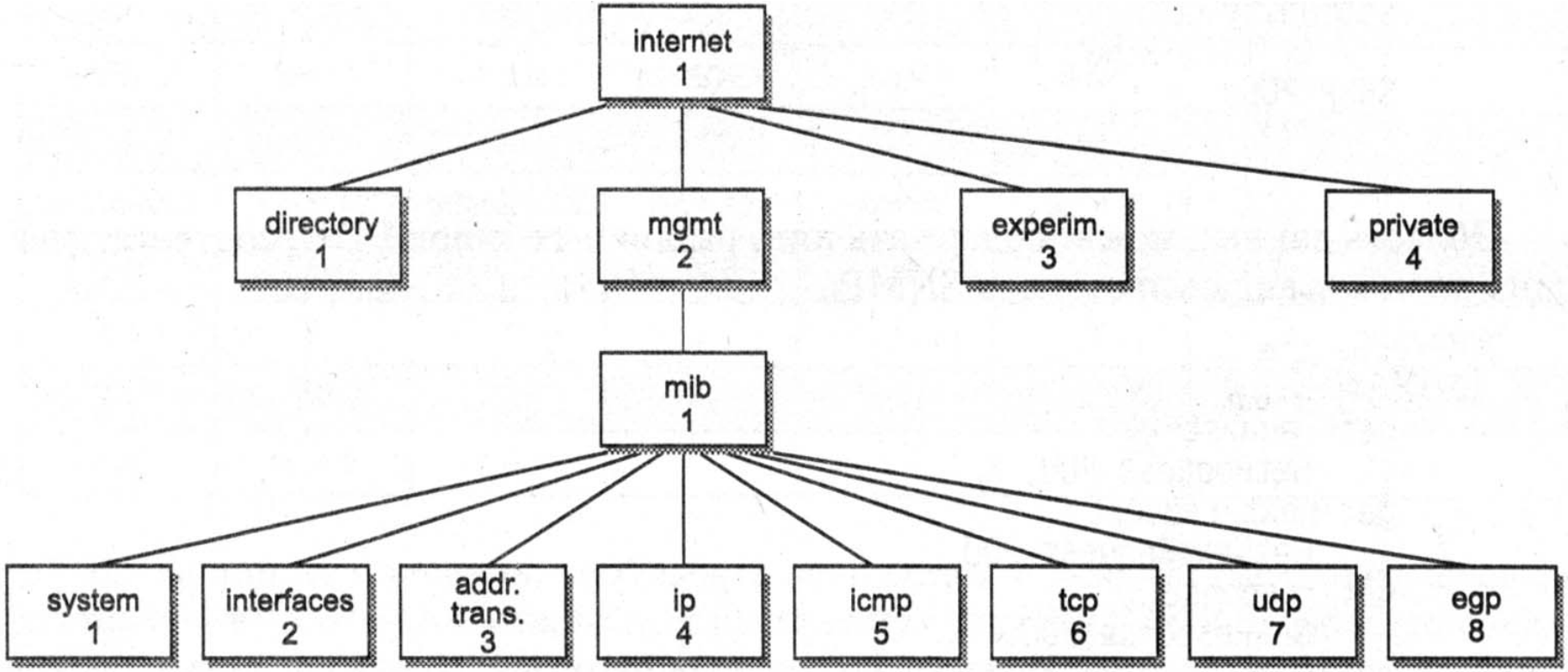
Иерархия идентифи-каторов объектов OSI



SNMP MIB-I, 8 групп

1. System
2. Interfaces
3. Address Translation Table
4. IP
5. ICMP
6. TCP
7. UDP
8. EGP

Часть дерева ISO, объекты MIB-I



Пример: iso(1).org(3).dod(6).internet(1).mgmt(2).mib(1).system(1).sysUpTime(3)

Спецификация RMON-MIB (N16)

- Statistics - тек. данные
- History - сохраненные данные
- Alarms - значения
- Hosts
- HostTopN
- TrafficMatrix - попарная интенсивность (таблица)
- Filter - условия
- PacketCapture - условия
- Event -условия

SNMPv2 : типы сообщений

Тип SNMP-сообщения	Функция
GetRequest GetNextRequest GetBulkRequest	Менеджер-агенту: получить данные, следующие, блок)
InformRequest	Менеджер-менеджеру: передать MIB-значение
SetRequest	M-A: задать MIB значение
Response	A-M: ответ на запрос значением
Trap	A-M: оповещение M

SNMP модели безопасности

- SNMPv1
  - Community-based модель безопасности: (private (rw), public(r))
- SNMPv2
  - v2p — Party-based Security Model. Party – логическая сущность, определяющая конкретный протокол аутентификации и протокол защиты/шифрации данных.
  - v2c — Community-based Security Model
  - v2u — User-based Security Model
- SNMPv3
  - USM User-based Security Model
  - View-Based Access Control Model (VACM): определяет конкретный набор объектов MIB, к которым может быть доступ со стороны конкретной группы и в конкретном контексте. Т.о. администратор определяет какая и кому информация доступна.
  - Определены три уровня:
  - noAuthNoPriv – no authentication and no privacy password;
  - authNoPriv – authentication, but no privacy password;
  - authPriv - authentication, and privacy password.

SNMP security and administration

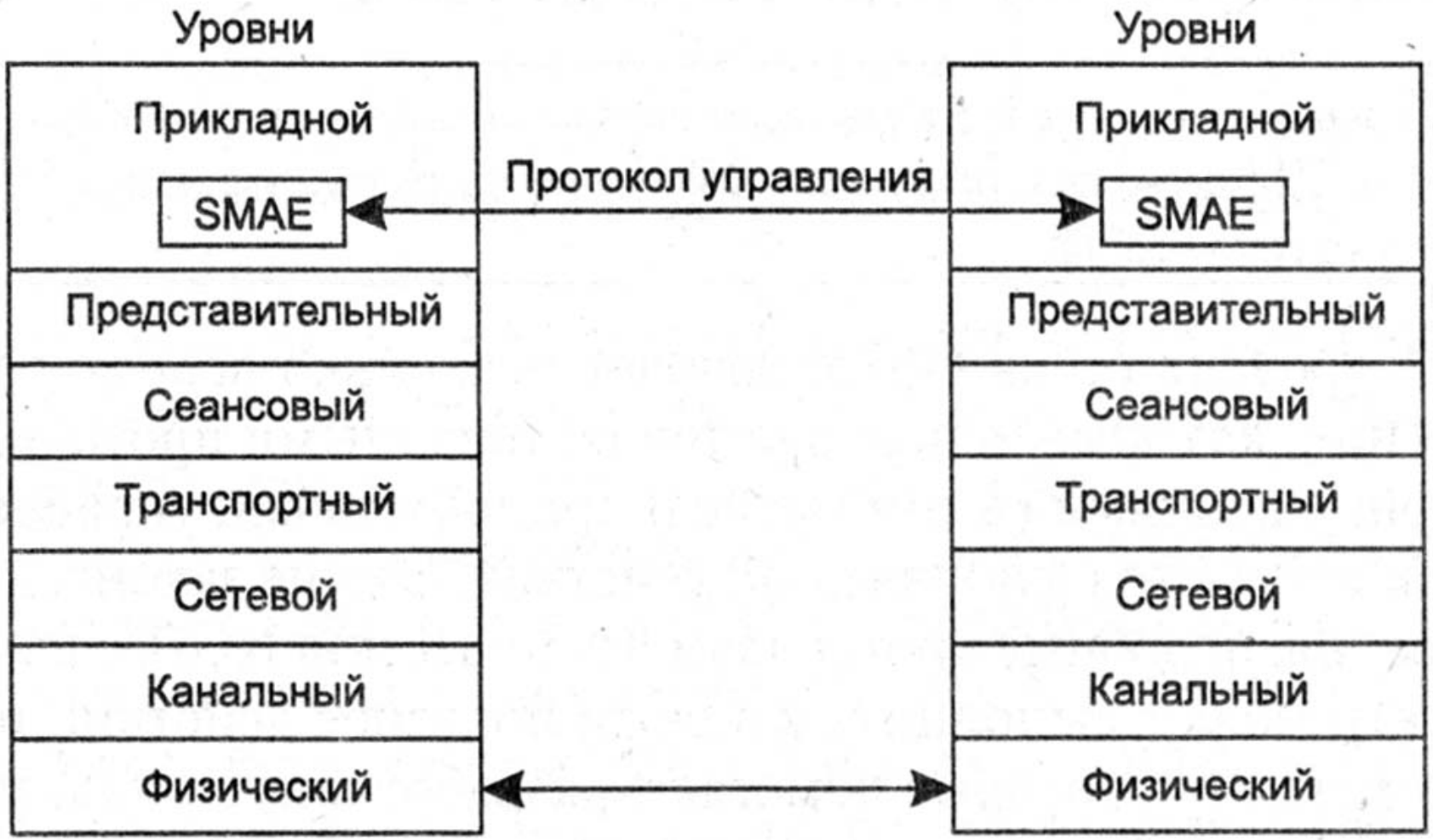
- encryption: DES-encrypt SNMP message
- authentication: compute, send MIC(m,k): compute hash (MIC) over message (m), secret shared key (k)
- protection against playback: timestamps
- view-based access control
  - SNMP сущность поддерживает БД прав доступа и политик для различных пользователей
  - БД сама представляет собой объект управления

SNMPv3 security features

- Encryption. SNMP PDUs can be encrypted using the Data Encryption Standard (DES), the secret key of the user encrypting data must be known at the receiving entity.
- Authentication. SNMP combines the use of a hash function, such as the MD5, with a secret key value to provide both authentication and protection against tampering. The approach, known as HMAC (Hashed Message Authentication Codes).
  - m - SNMP PDU, that sender wants to send to the receiver, have already been encrypted.
  - Both the sender and receiver know a shared secret key, K
- The sender will send Message Integrity Code (MIC), MIC(m,K) over the combined PDU and key which then transmitted along with m. When the receiver receives m, it appends the secret key K and computes MIC(m,K). If this computed value matches the transmitted value of MIC(m,K) then the receiver knows also that the message was sent by someone who knows the value of K, i.e., by a trusted, and now authenticated, sender.
- Protection against playback. The sender includes a value in each message, based on a counter in the receiver. This counter reflects the amount of time since the last reboot of the receiver's NM software and the total number of reboots since the receiver's NM software was last configured. As long as the counter in a received message is within some margin of error from the receiver's actual value, the message is accepted as a non-replay message.
- Access control. SNMPv3 provides a view based access control (VBAC), which controls which network management information can be queried/set by which users. An SNMP entity stores information about access rights and policies in a Local Configuration Datastore (LCD). Portions of the LCD are themselves accessible as managed objects, and thus can be managed and manipulated remotely via SNMP.

SNMPv3, 1999г.

Субъекты системы управления OSI: System Management Application Entities (SMAE)



Аппаратно-программные платформы администрирования

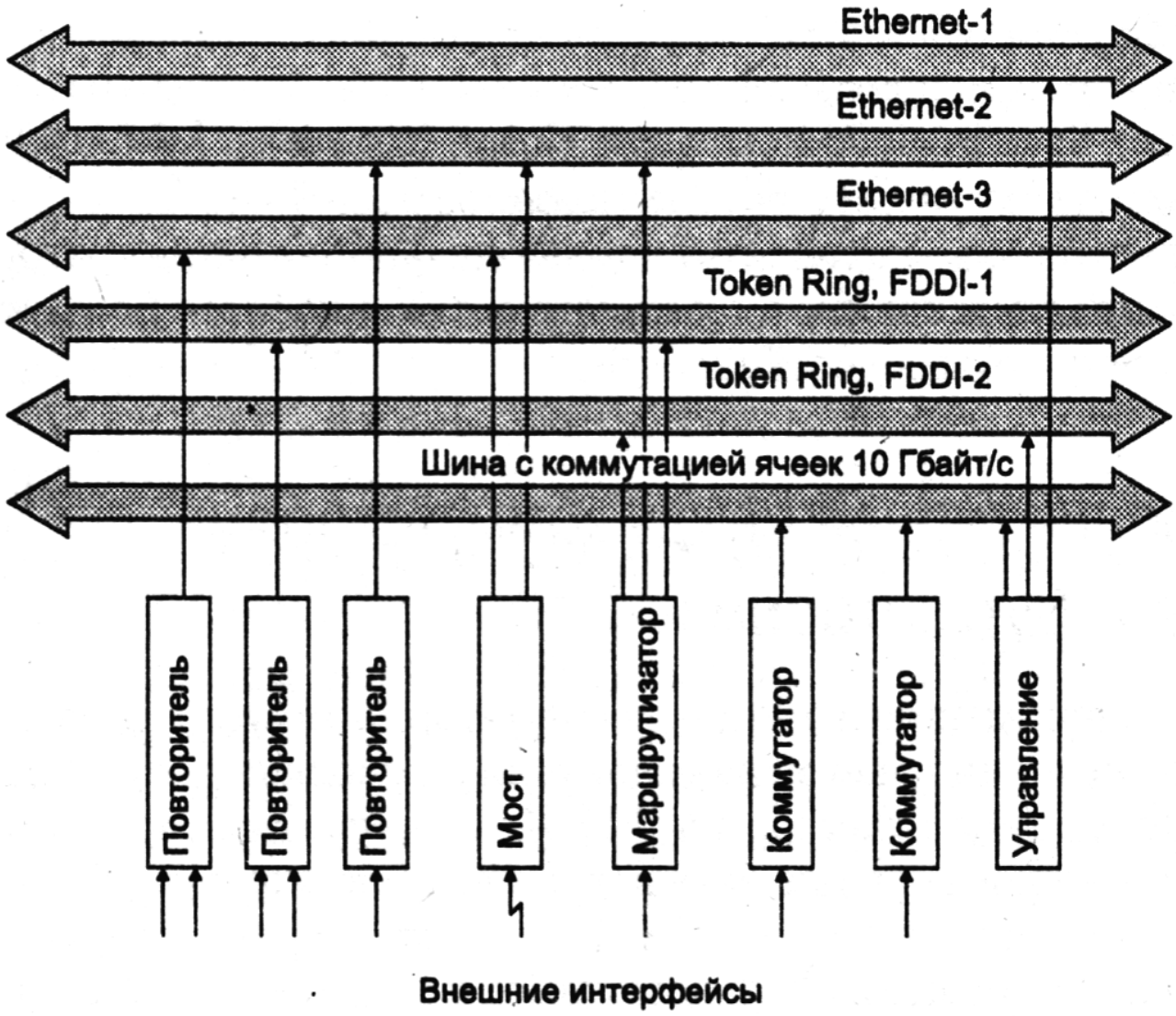
- MS IntelliMirror – набор технологий управления ИТ-инфраструктурой снижающих т.н. стоимость эксплуатации (total cost of ownership, TCO)
- IBM Tivoli – ПО управления ИТ-инфраструктурой предприятия и обеспечения безопасности

ПО MS IntelliMirror

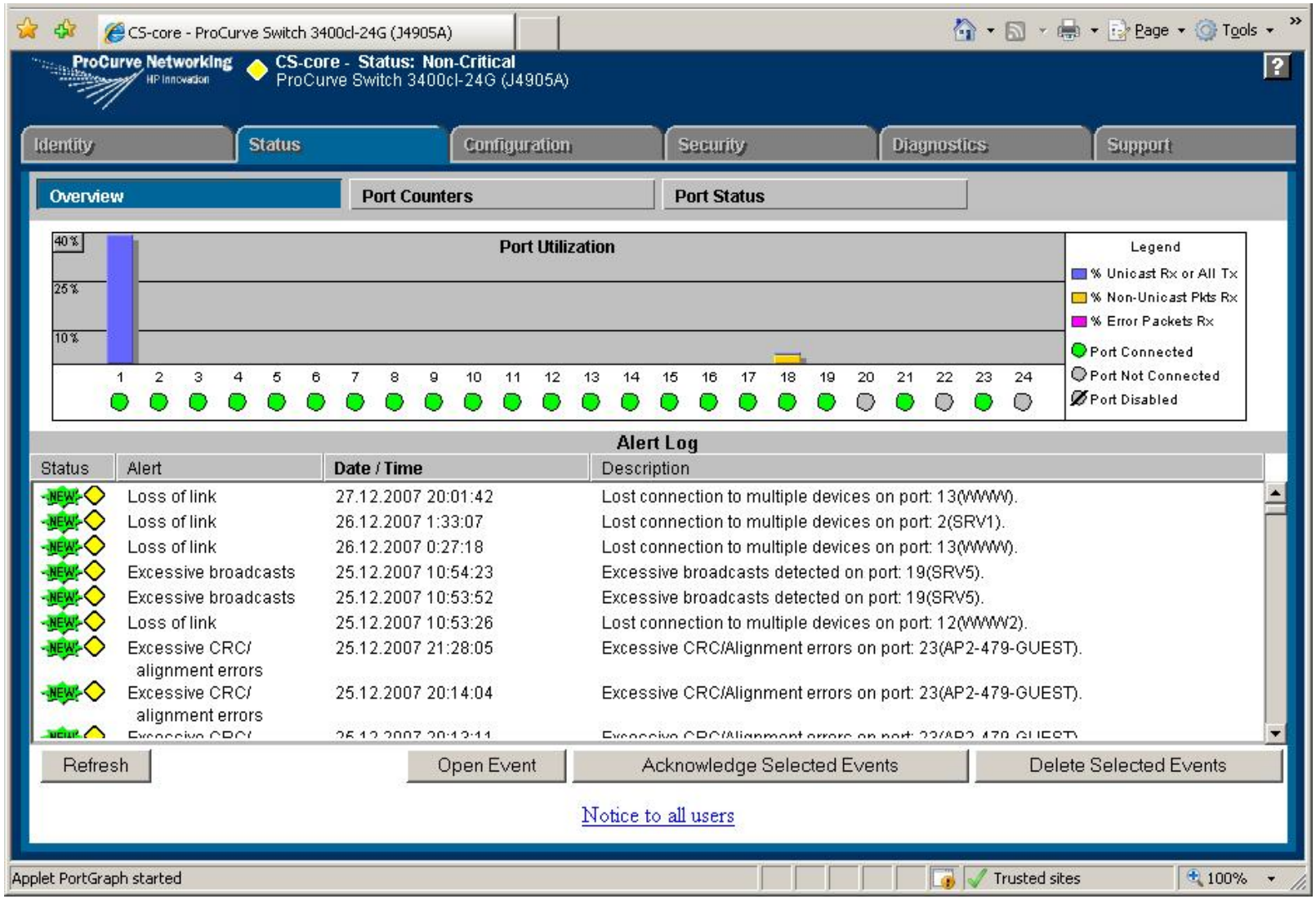
- Возможности IntelliMirror
  - Управление данными (Data Management)
    - перенаправление каталогов (Folder Redirection)
    - автономные файлы (Offline Folders)
    - дисковые квоты
  - Управление пользовательскими параметрами настройки (Desktop Settings Management)
  - Установка и сопровождение ПО (Software Installation and Maintenance)
  - Службы удаленной установки (RIS)
- Технологии, входящие в состав IntelliMirror
  - Служба каталогов Active Directory
  - Групповая политика Group Policy
  - Перемещаемые профили пользователя Roaming User Profiles
  - Перенаправление каталогов Folder Redirection
  - Автономные файлы Offline Folders

Администрирование корпоративных коммутаторов

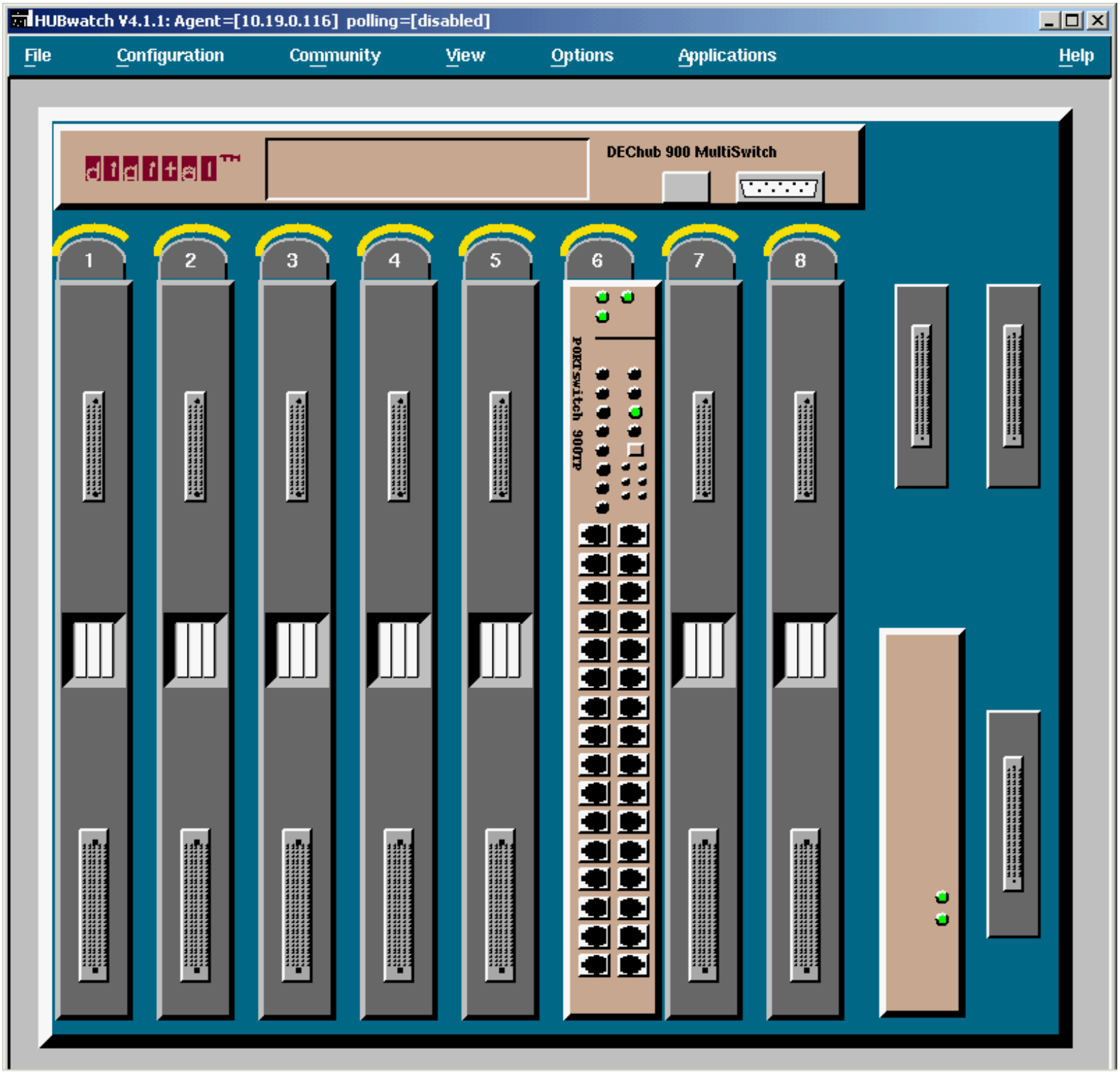
- SNMP
- HTTP
- CLI/SS



HTTP интерфейс управления



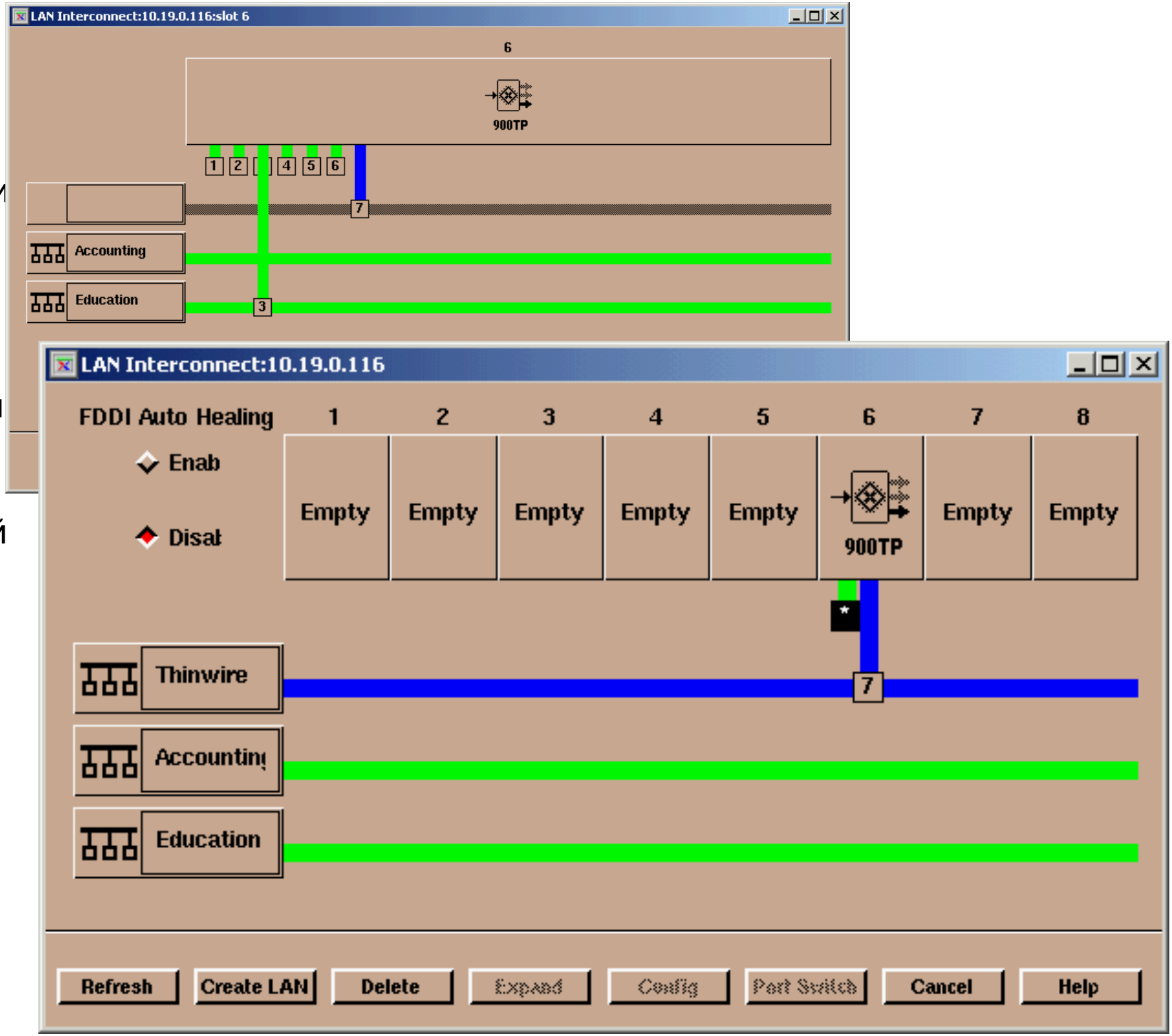
ПО управления сетевым оборудованием DEC_NRG HubWatch. Используется SNMP. Показан вариант для X-Window, OSF/Digital Unix



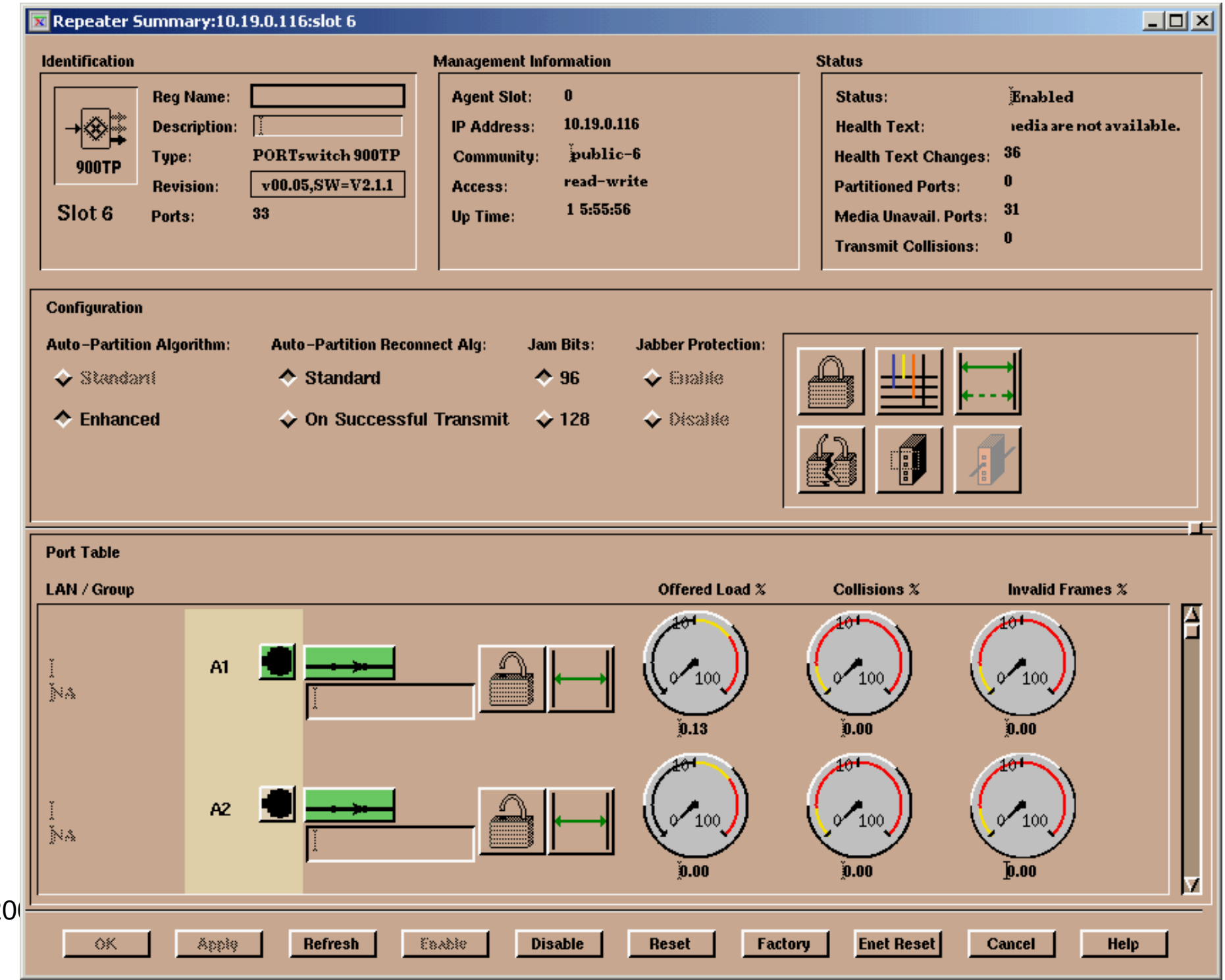
04.09.2002

ПО управления сетевым оборудовани ем DECNRG HubWatch.

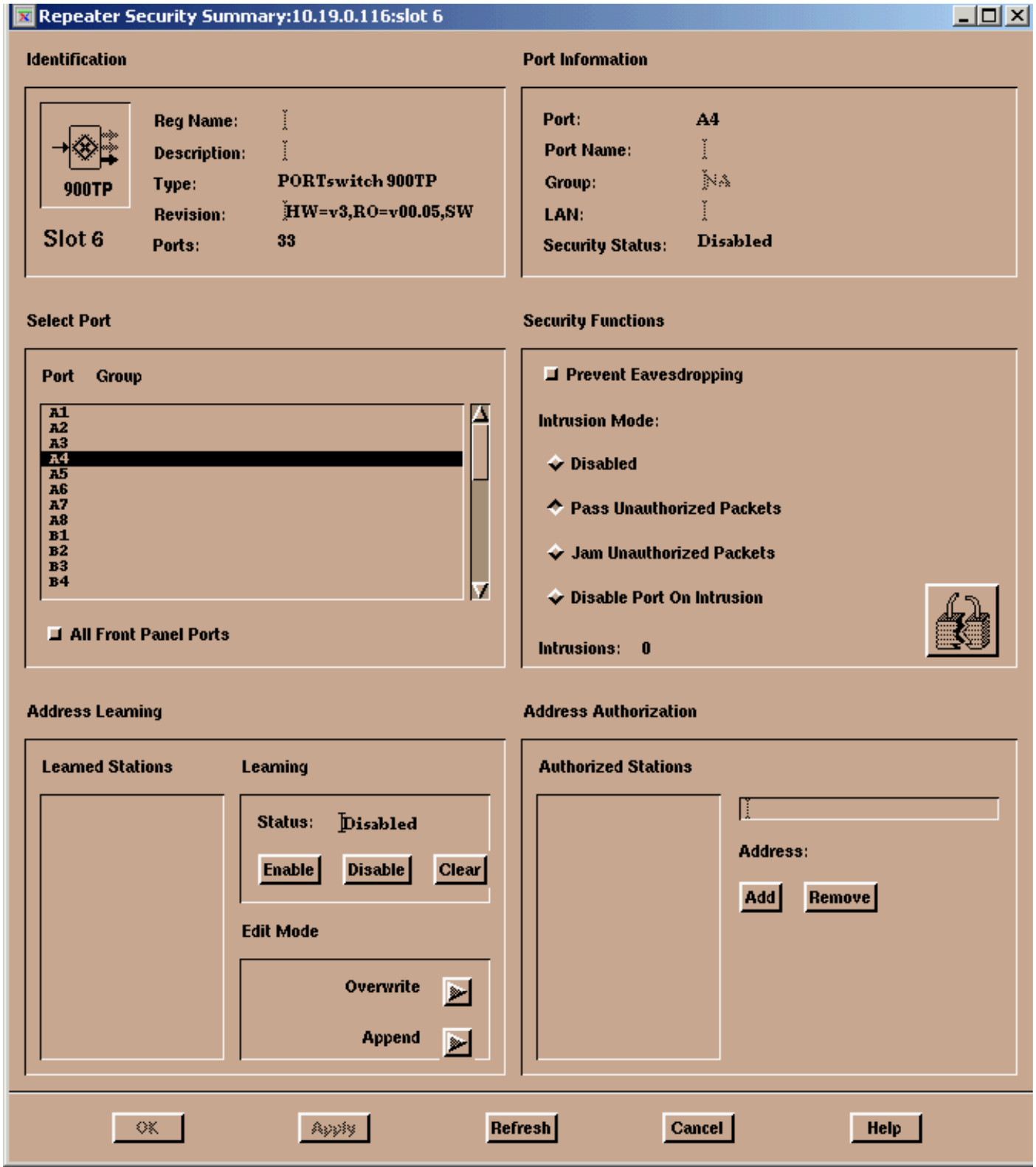
Соединения модулей с помощью магистралей платформы MultiSwitch.



Панель управления репитером PortSwitch

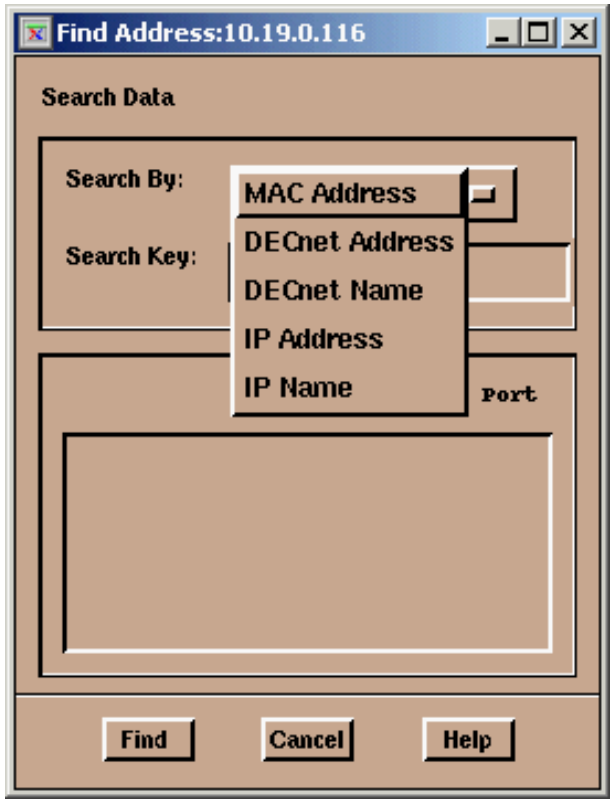


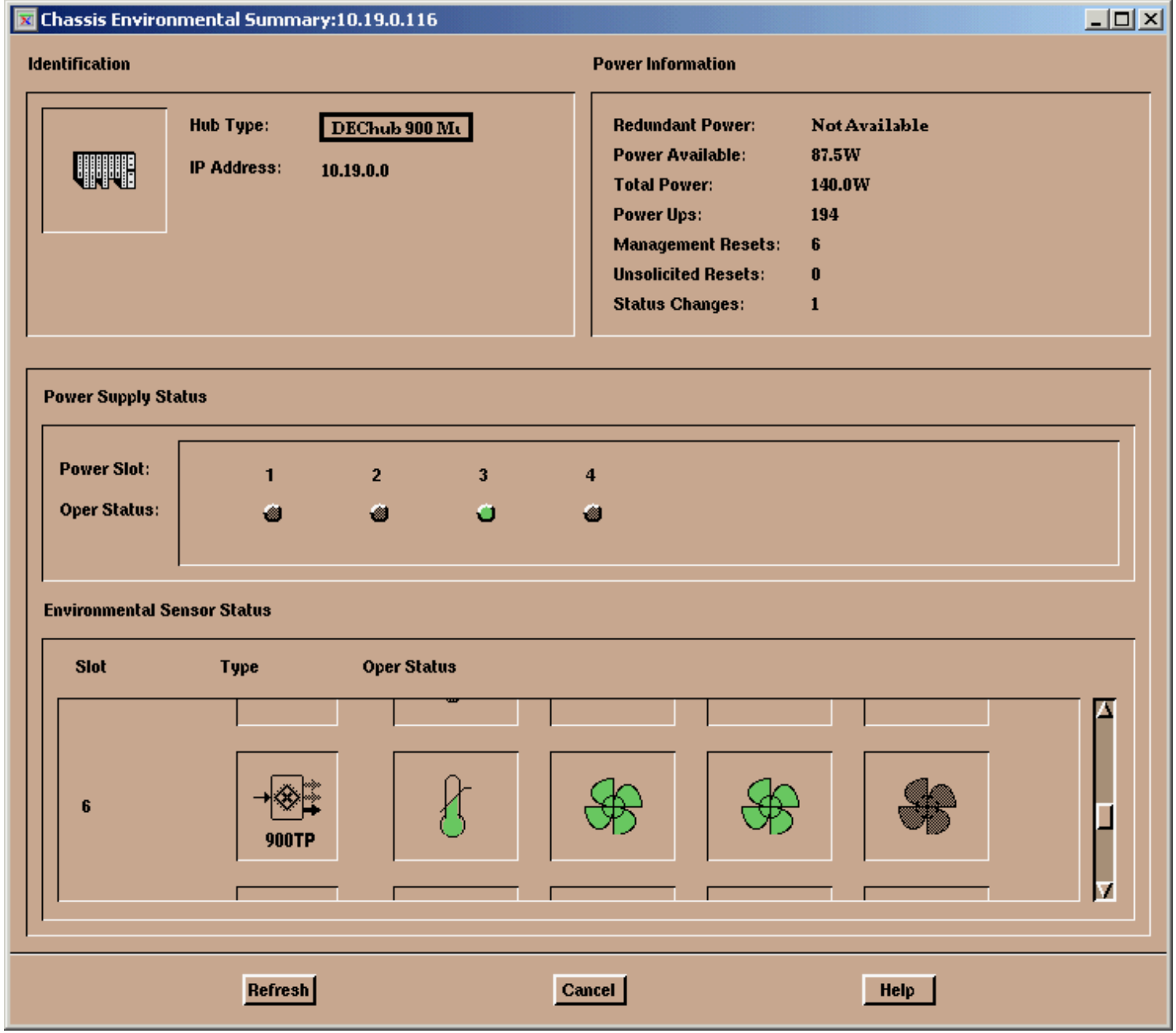
Управление параметрами безопасности репитера



04.09.2002

Обзор температурного состояния шасси. Утилиты поиска шасси.





Интеллектуальные системы управления физическим уровнем

- Интеллектуальные системы управления физическим уровнем – Intelligent Physical Layer Management Solution (IPLMS)
- См. BYTE за №3/2004 «Системы управления СКС в реальном времени»
- http://www.cs.vsu.ru/~kas/doc/admis/RTCMS.pdf

IBM Tivoli – ПО управления ИТ-инфраструктурой предприятия

- to be continued …