Immune Phase 2
Web-Based Network Management

September 2, 1999

Jean-Philippe Martin-Flatin and Jean-Pierre Hubaux
Swiss Federal Institute of Technology, Lausanne
Institute for computer Communications and Applications
ICA
martin-flatin@epfl.ch hubaux@ica.epfl.ch
http://icawww.epfl.ch

Outline

- Problems with SNMP-based network management
- Proposed solution:
  - Web-based network management (HTTP, Java applets and servlets)
  - push model for regular management
  - pull model for *ad hoc* management
- Overview of JAMAP
- Demo

Problems with NMPs

- For customers:
  - too expensive (hardware and software)
    - ➠ dedicated hardware
  - limited support for third-party RDBMSs
  - investment bound to processor & operating system
- For network equipment vendors:
  - the support of device-specific add-ons is too expensive:
    - ➠ many NMPs, many OSs, and many add-ons
- For customers and network equipment vendors:
  - poor time-to-market for add-ons, depending on market share
  - MIB versioning

Problems with SNMP

- SNMP expertise is scarce and expensive (esp. SNMPv3)
- Scalability, network overhead and latency are adversely affected by some early protocol design decisions (SNMPv1):
  - BER encoding, SNMP table retrieval, OIDs are verbose, no compress.
- Low-level semantics:
  - instrumentation MIBs, site-specific network applications developed from scratch
  - bound to an NMP API, not a technology
- Security
- Unreliable transport protocol
- Distribution: M2M MIB obsolete, Script MIB not used yet
- Evolution hampered by legacy syst.: “better replace than repair”

Proposed Solution (1/2)

- Keep:
  - MIBs
  - organizational model
- Change management framework:
  - pull model --> push model for repetitive tasks
  - move some workload from the manager to the agents
- Change communication protocol:
  - SNMP --> HTTP
  - connectionless UDP --> persistent TCP connections
  - `gzip` compression
  - unlimited number of MIB variables per push cycle
  - BER encoding --> MIME parts + {strings, XML, ser. Java objects...}
  - natural table retrievals

Proposed Solution (2/2)

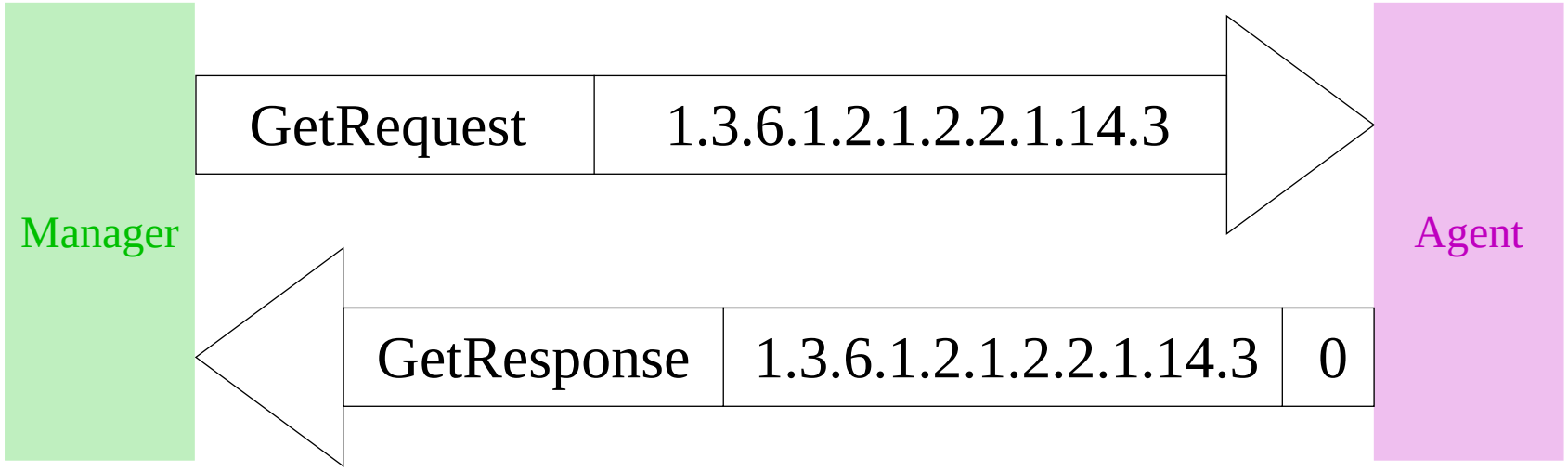
- Change NMP:
  - split manager (from 2-tier to 3-tier architecture):
    - management server (Java servlets)
    - management station (Web browser)
  - rewrite manager code: expensive binary software --> less expensive Java software (indep. of OS and proc., no RDBMS-specific glue code)
  - expensive specific add-ons --> less expensive standard Java applets
  - dedicated NMP hardware --> any hardware
  - few third-party RDBMSs --> any RDBMS via JDBC
  - distribution made easier:
    - manager: monolithic NMP --> distributed servlets
    - manager to manager: standard distributed Java application (future work)
    - manager to agent (mobile code): object serialization (future work)

Why HTTP Between Agents and Managers?

- Four techniques to distribute a Java application:
  - HTTP
  - sockets
  - RMI
  - Java IDL (CORBA)
- Distributed objects in network management (RMI or CORBA):
  - telecoms world = yes
  - IP world = no (maybe later: EmbeddedJava & lightweight RMI)
- HTTP > sockets:
  - natural communication between servlets within the mgmt server
  - same technology within the server and between agents and server
  - firewall setup easier for nonexperts (e.g. Web server = mgmt server)

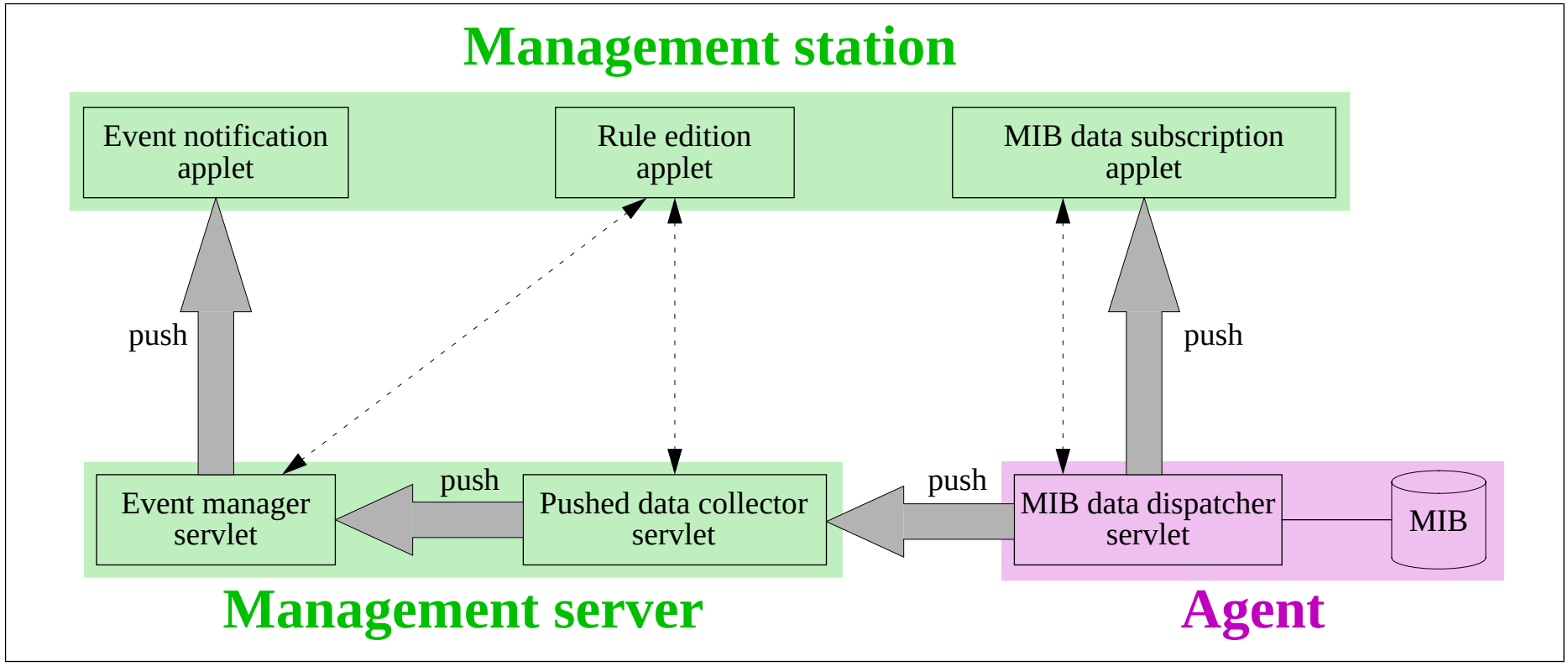
Why Use Push Technologies?

- Save bandwidth: decrease network overhead of mgmt data
- Example: error rate for inbound traffic through interface #3

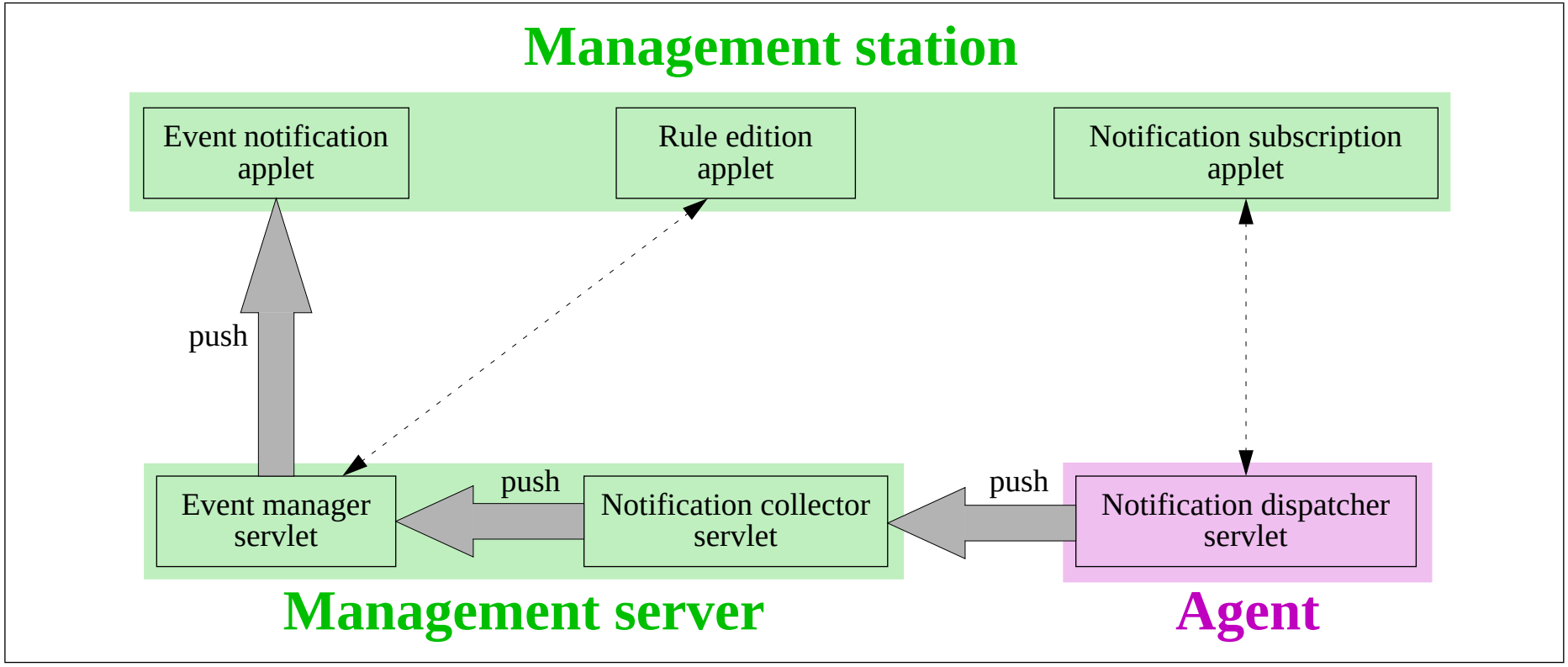


- Move some load from the manager to the agents
- Pave the way to Management by Delegation:
  - delegate preprocessing to the agents

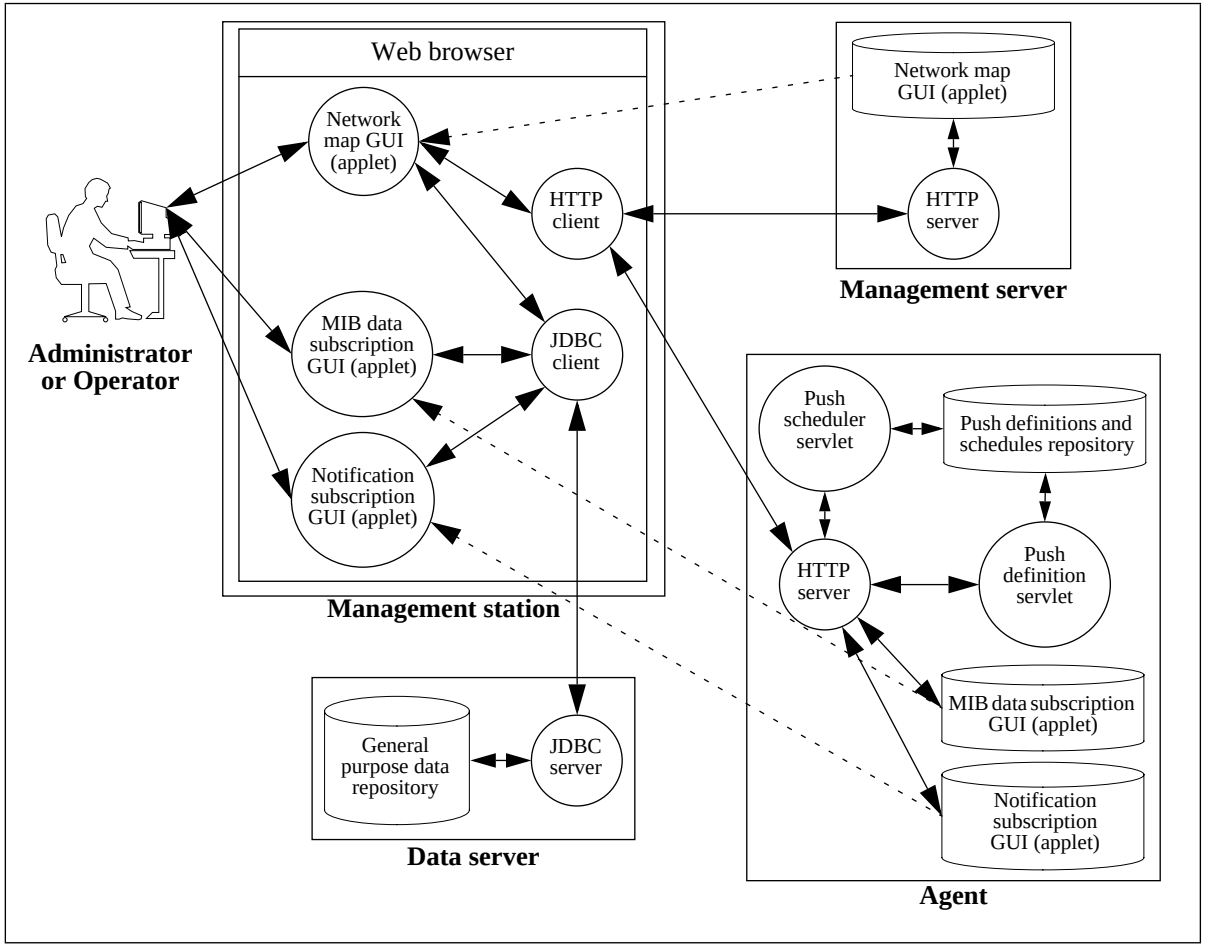
JAMAP: Monitoring and Data Collection



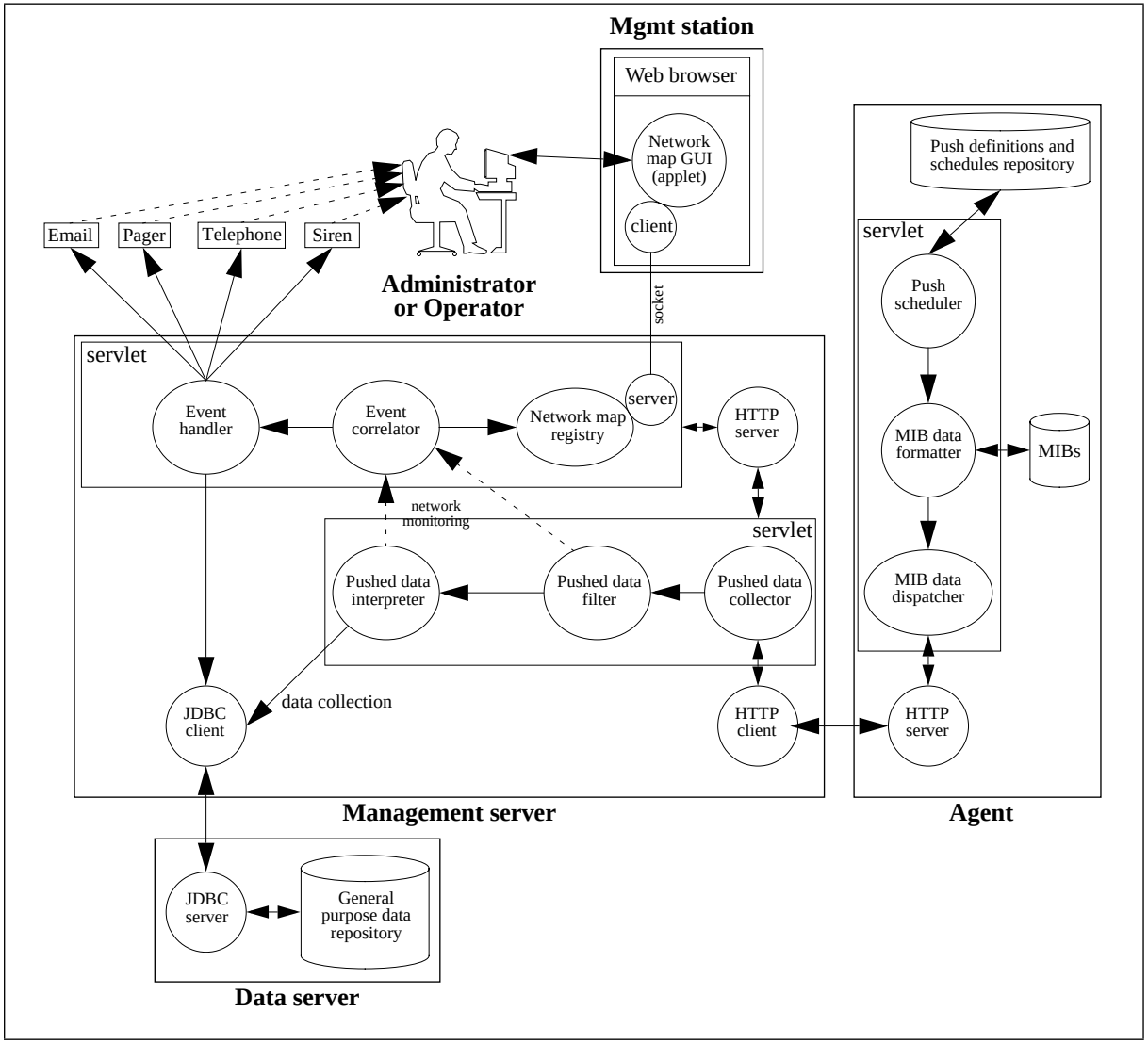
JAMAP: Notifications



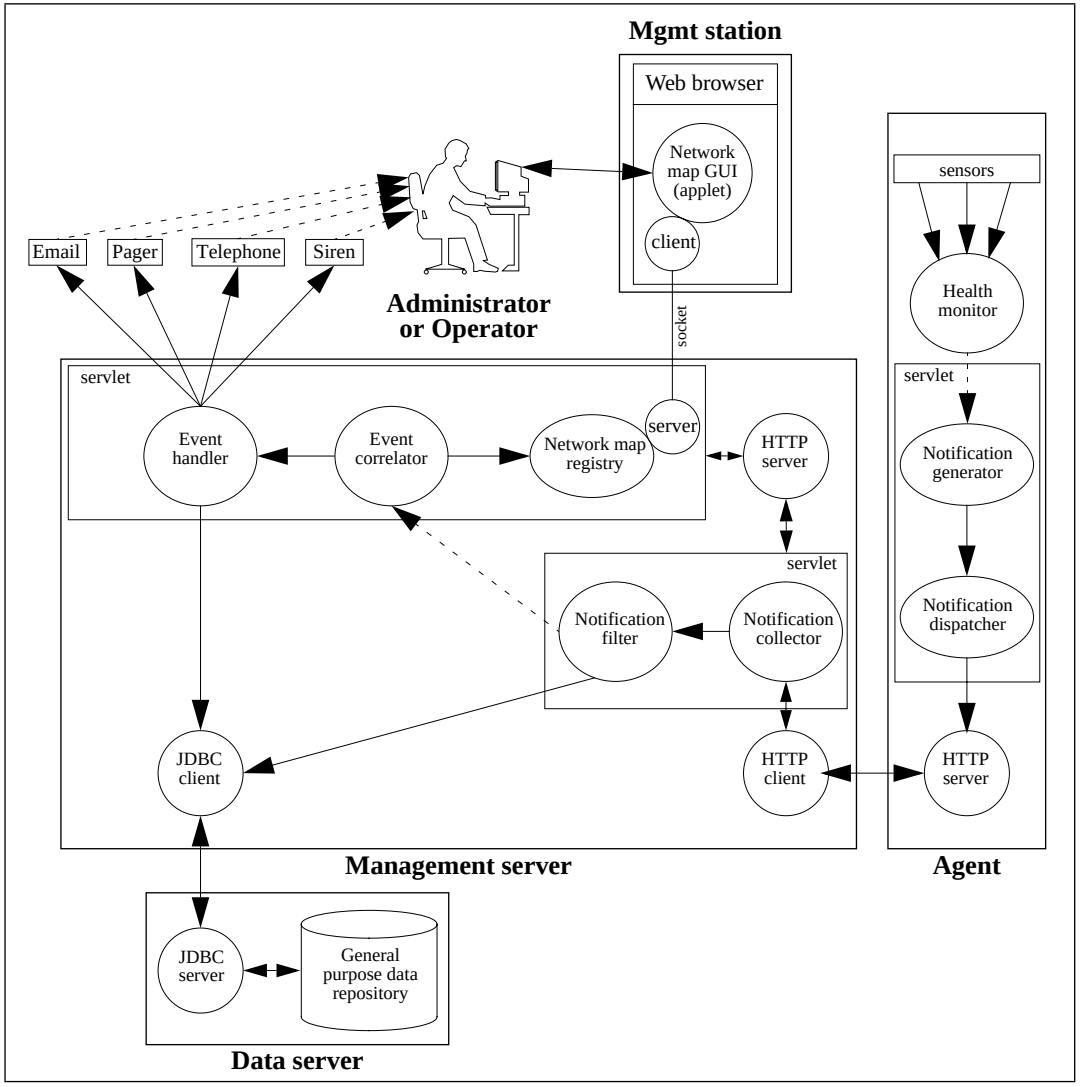
Publication and Subscription Phases



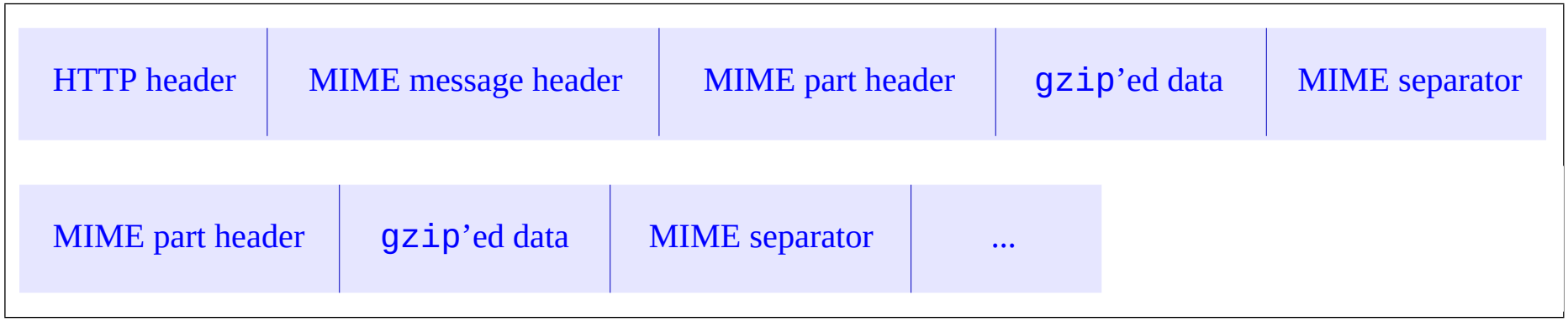
Push-Based Distribution for Monitoring and Data Collection



Push-Based Distribution for Notifications



HTTP and MIME



MIME = Multipurpose Internet Mail Extensions

- Advantages:
  - simple to implement
  - firewalls: minor change (assuming Web access already)
- Drawbacks:
  - the manager must detect a network outage to set up a new connection:
    - ➠ send keepalives if no data after 9 minutes
    - ➠ blind during 9 minutes, or send keepalives more often

Conclusions (1/2)

What do we gain by going from SNMP-based pull to Java-based push to manage IP networks?

- Get rid of the expensive NMP
- Use well-known Web technologies instead of domain-specific SNMP
- Reduce network overhead of management data
- Reduce development costs of add-ons
- Zero the time-to-market of add-ons (embedded)
- Put small and large equipment vendors in fair competition w.r.t. integrated management
- Simplify the management of remote subsidiaries across a firewall
- Improve the support for third-party RDBMSs
- Remain backward compatible by using proxies for legacy systems

Conclusions (2/2)

What does it cost to go from SNMP-based pull to Java-based push to manage IP networks?

- network equipment vendors must add software to their equipment:
  - HTTP server (usually done today)
  - push system
  - scheduling system
  - JDK (JVM)
- administrators need to synchronize the clocks of the managers and the agents (e.g. with NTP)
- we need professional-grade software for the manager:
  - more and more vendors in the Web-based management market