RFID: Technology and Applications

Sridhar Iyer

IIT Bombay

sri@it.iitb.ac.in

www.it.iitb.ac.in/~sri

Outline

- Overview of RFID
  - Reader-Tag; Potential applications
- RFID Technology Internals
  - RF communications; Reader/Tag protocols
  - Middleware architecture; EPC standards
- RFID Business Aspects
- Security and Privacy
- Conclusion

Product Marketing – 75 years ago

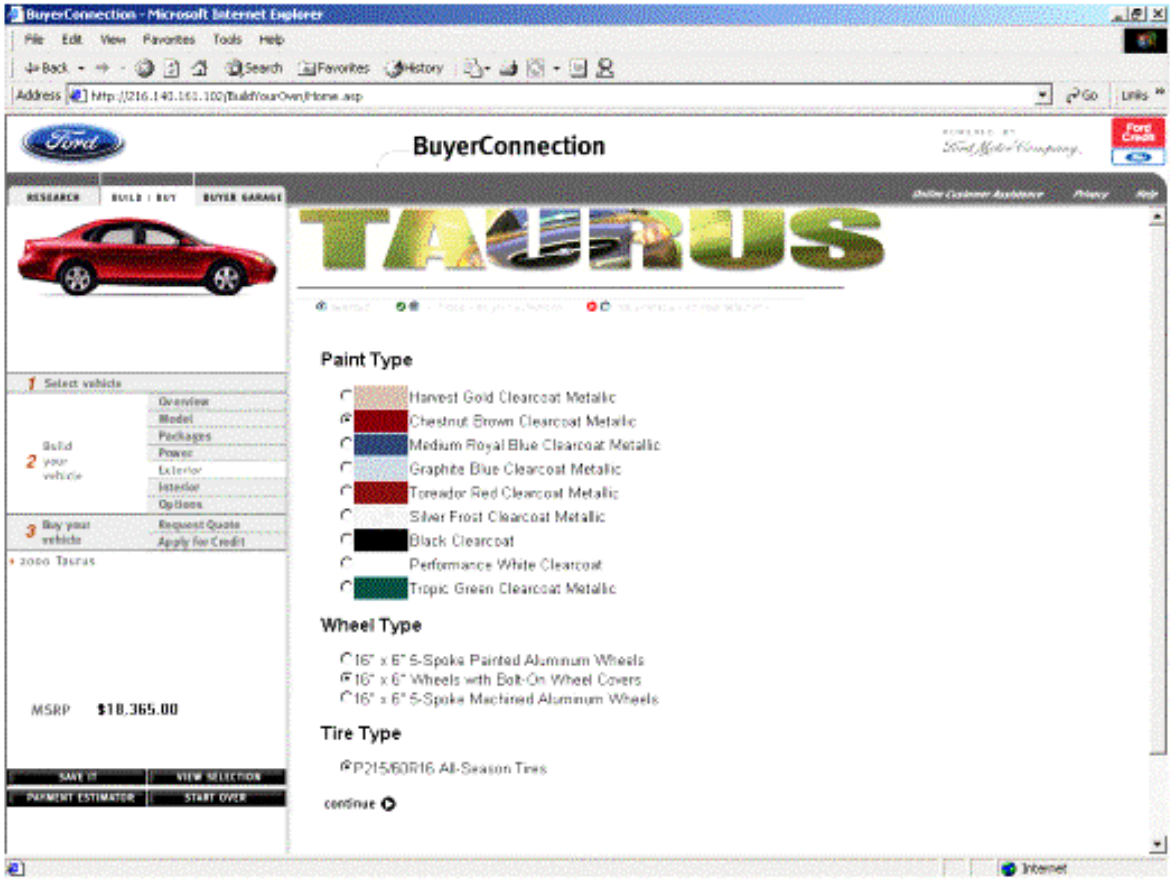
You can have any color, as long as its black !

4

Product Marketing - Today

Add consumer flexibility, courtesy of robotics, computers …

Customer window into final stage of manufacturing



Effect on manufacturing

- Need to ensure error-free, custom assembly
- Need inventory of components for the various customization options

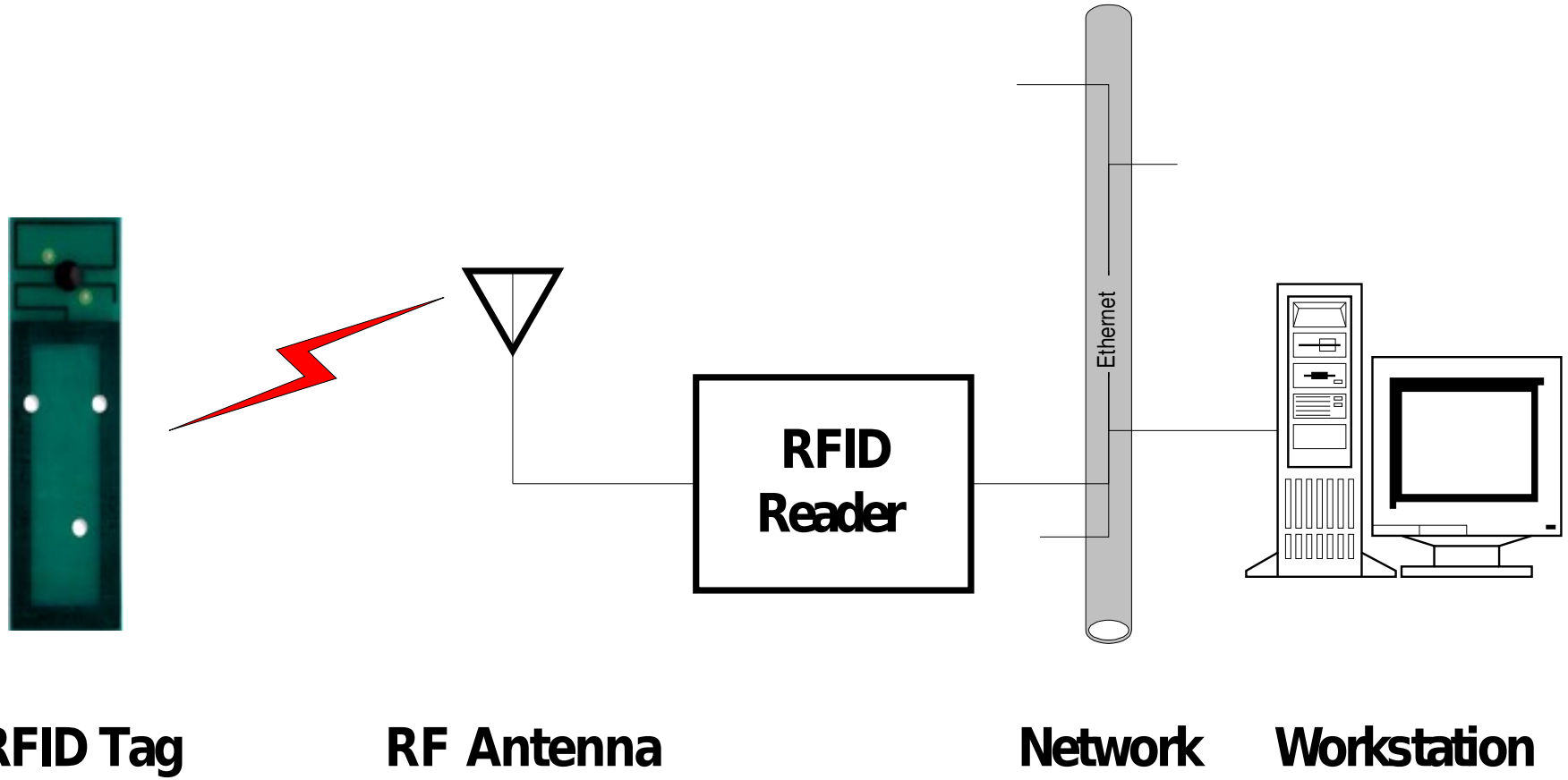
- Critical Issues
  - Assembly process control
  - Inventory management
  - Supply chain integration
  - Customer insight

- One solution: RFID

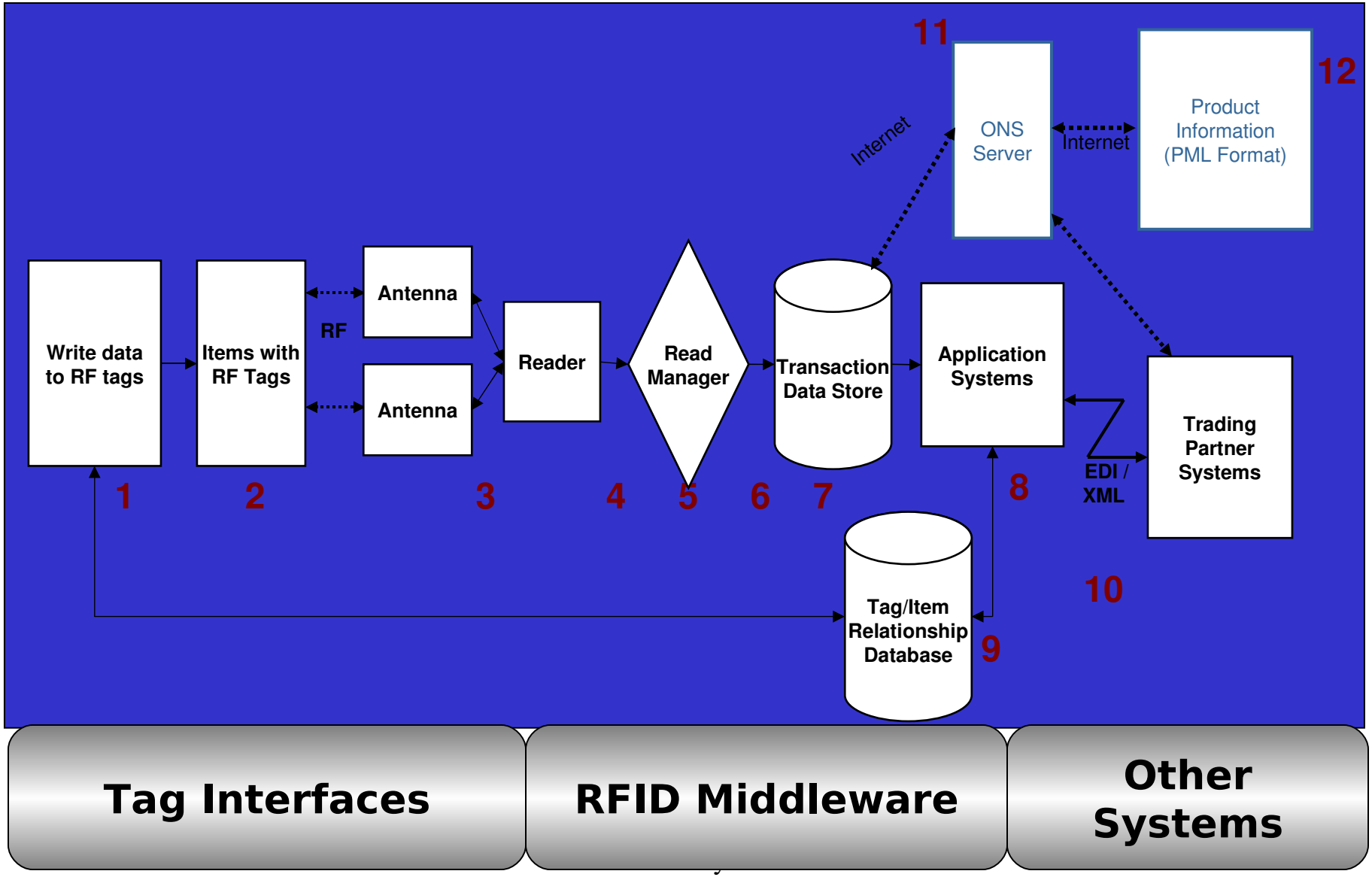
What is RFID?

- RFID = Radio Frequency IDentification.
- An ADC (Automated Data Collection) technology that:
  - uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize, track..
  - Is fast and does not require physical sight or contact between reader/scanner and the tagged item.
  - Performs the operation using low cost components.
  - Attempts to provide unique identification and backend integration that allows for wide range of applications.
- Other ADC technologies: Bar codes, OCR.

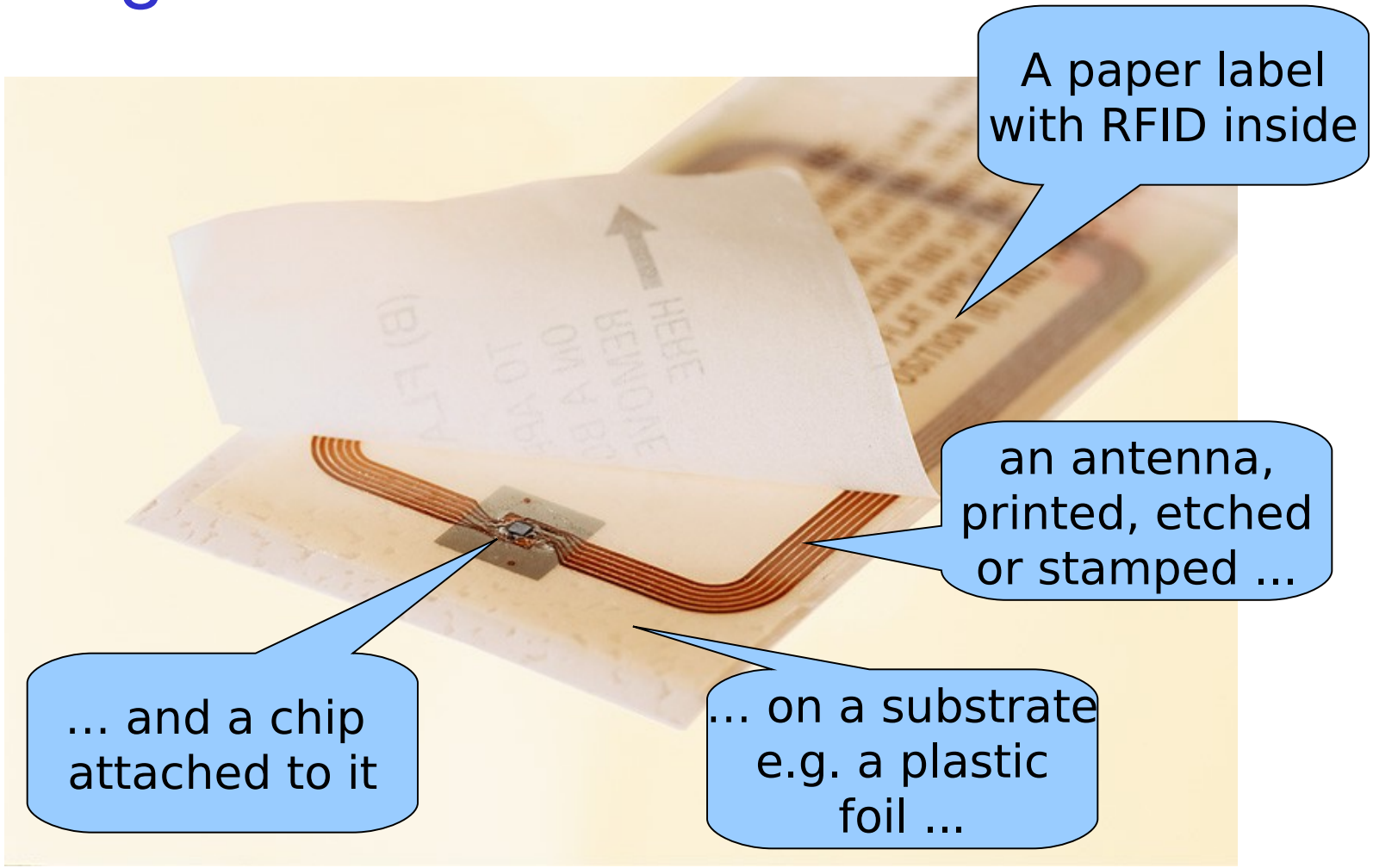
RFID system components



RFID systems: logical view

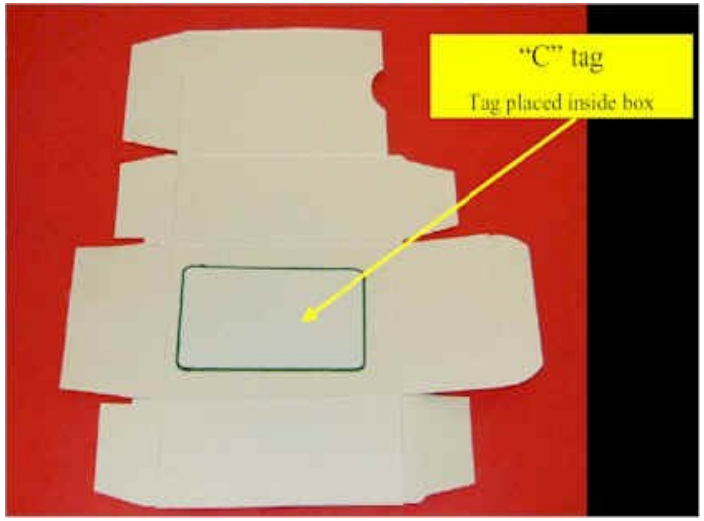


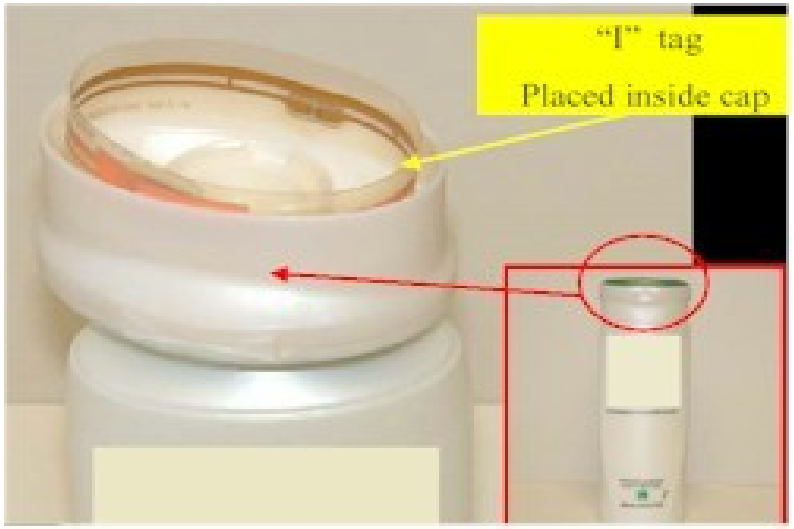
RFID tags: Smart labels



Source: **www.rfidprivacy.org**

Some RFID tags



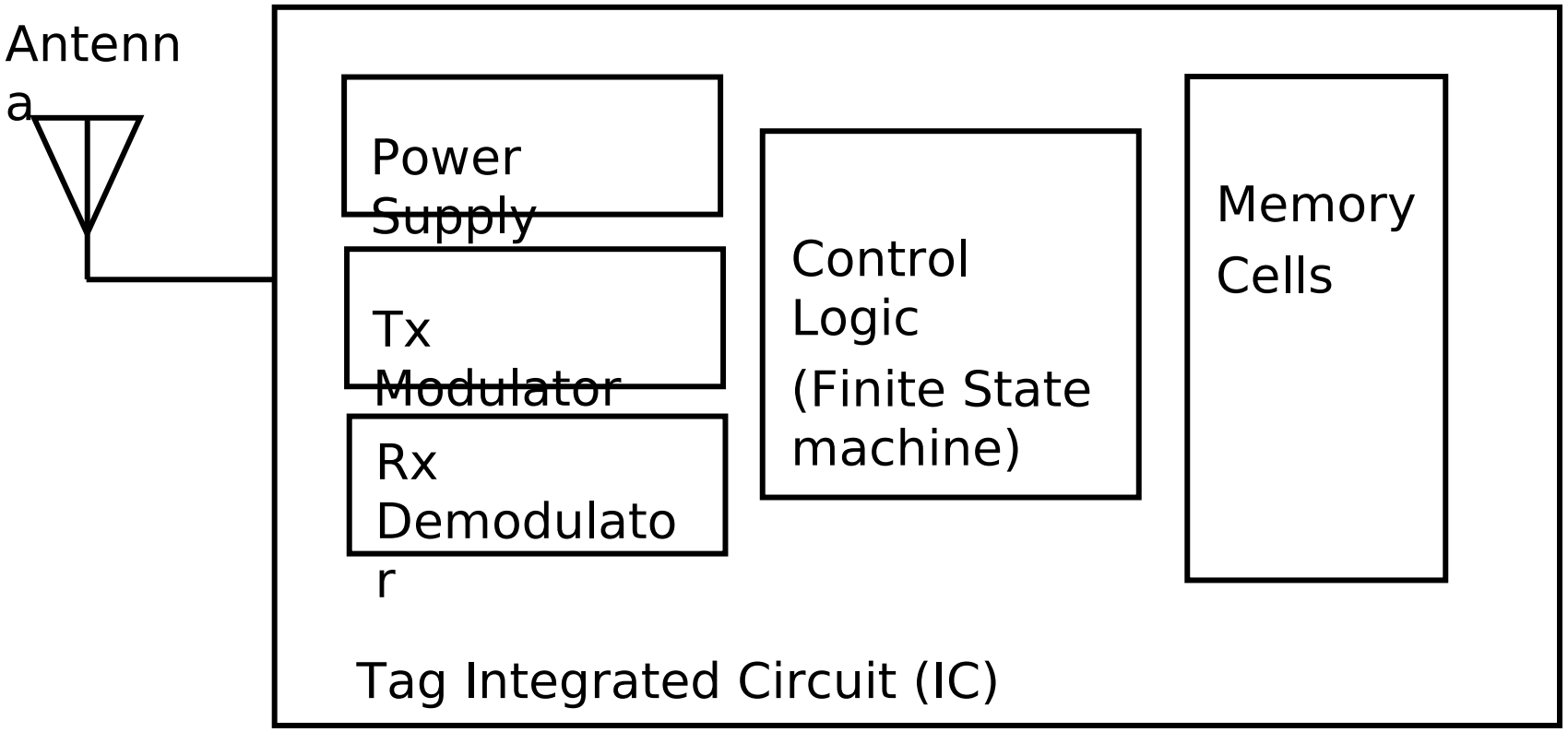


Source: **www.rfidprivacy.org**

RFID tags

- Tags can be attached to almost anything:
  - Items, cases or pallets of products, high value goods
  - vehicles, assets, livestock or personnel
- **Passive Tags**
  - Do not require power – Draws from Interrogator Field
  - Lower storage capacities (few bits to 1 KB)
  - Shorter read ranges (4 inches to 15 feet)
  - Usually Write-Once-Read-Many/Read-Only tags
  - Cost around 25 cents to few dollars
- **Active Tags**
  - Battery powered
  - Higher storage capacities (512 KB)
  - Longer read range (300 feet)
  - Typically can be re-written by RF Interrogators
  - Cost around 50 to 250 dollars

Tag block diagram



RFID tag memory

- Read-only tags
  - Tag ID is assigned at the factory during manufacturing
    - Can never be changed
    - No additional data can be assigned to the tag
- Write once, read many (WORM) tags
  - Data written once, e.g., during packing or manufacturing
    - Tag is locked once data is written
    - Similar to a compact disc or DVD
- Read/Write
  - Tag data can be changed over time
    - Part or all of the data section can be locked

RFID readers

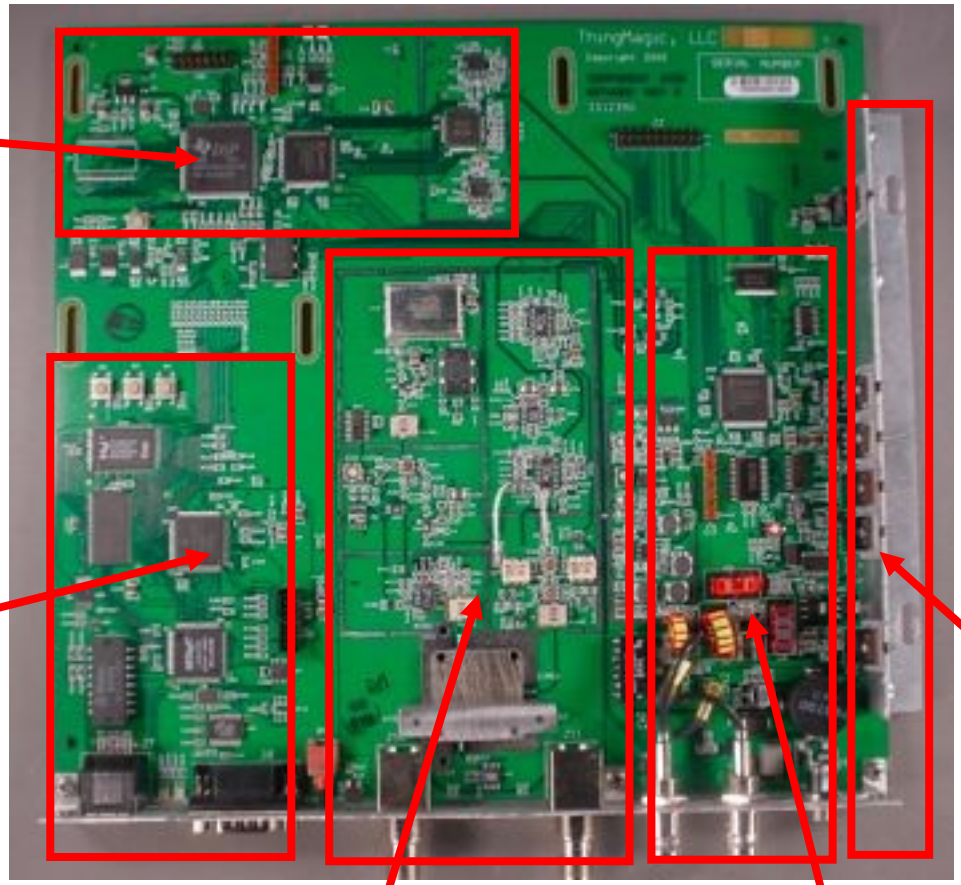
- Reader functions:
  - Remotely power tags
  - Establish a bidirectional data link
  - Inventory tags, filter results
  - Communicate with networked server(s)
  - Can read 100-300 tags per second

- Readers (interrogators) can be at a fixed point such as
  - Entrance/exit
  - Point of sale
- Readers can also be mobile/hand-held

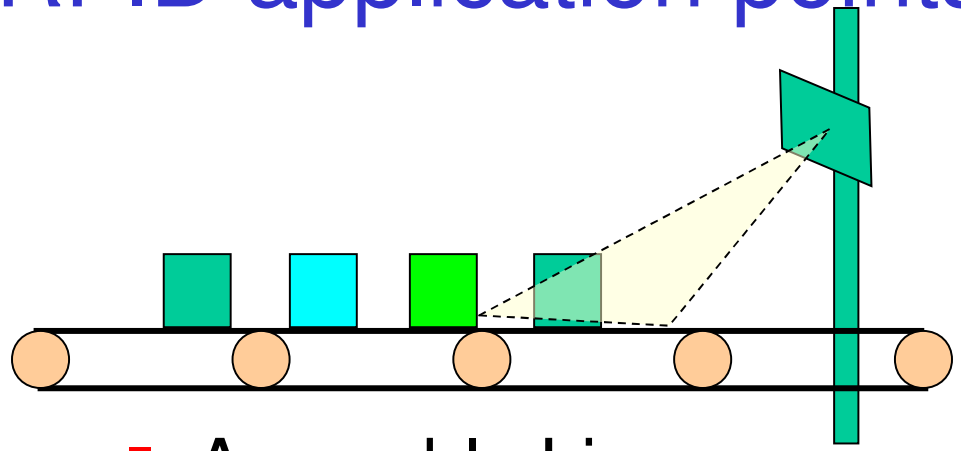
Some RFID readers

Source: **www.buyrfid.org**

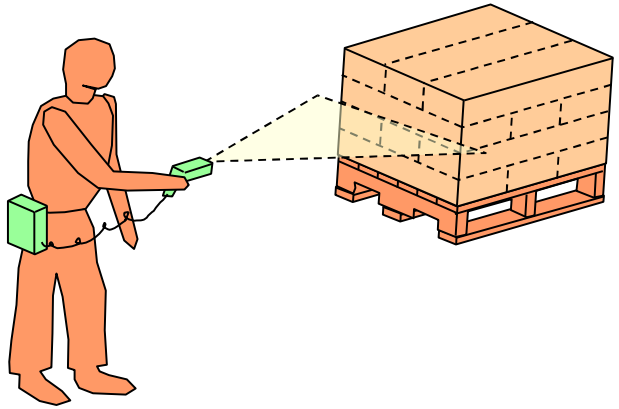
Reader anatomy



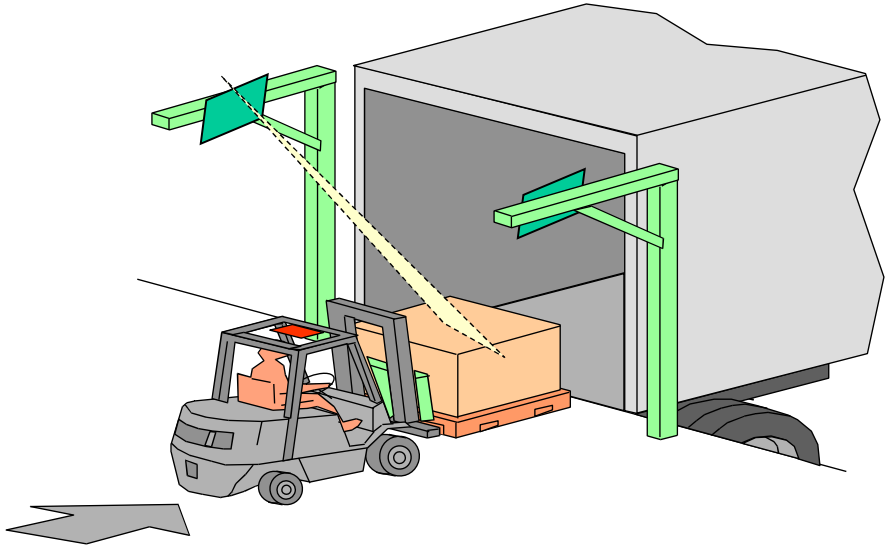
RFID application points



- Assembly Line



- Handheld Applications



- Shipping Portals

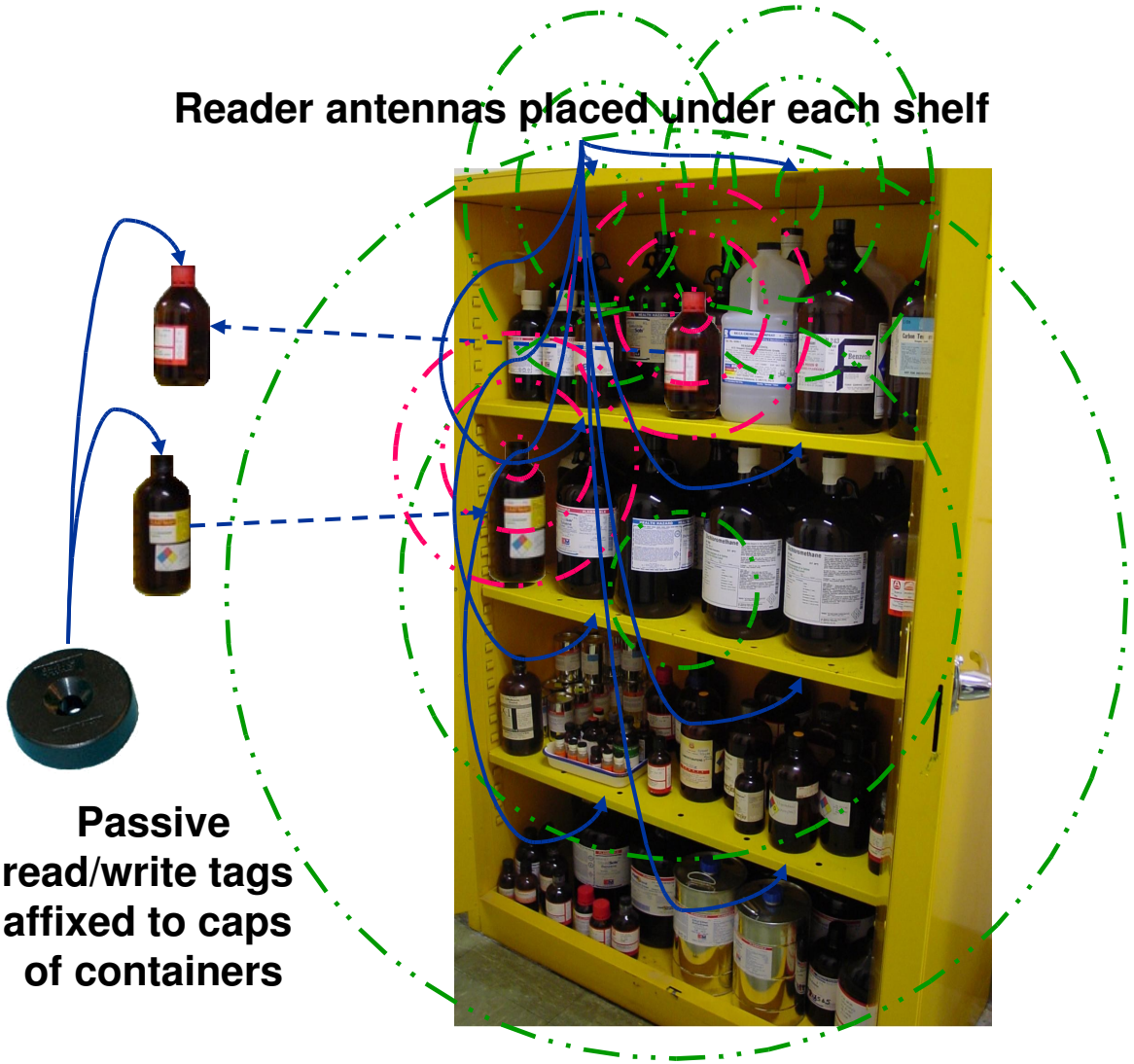
RFID applications

- Manufacturing and Processing
  - Inventory and production process monitoring
  - Warehouse order fulfillment
- Supply Chain Management
  - Inventory tracking systems
  - Logistics management
- Retail
  - Inventory control and customer insight
  - Auto checkout with reverse logistics
- Security
  - Access control
  - Counterfeiting and Theft control/prevention
- Location Tracking
  - Traffic movement control and parking management
  - Wildlife/Livestock monitoring and tracking

Smart groceries

- Add an RFID tag to all items in the grocery.
- As the cart leaves the store, it passes through an RFID transceiver.
- The cart is rung up in seconds.

Smart cabinet



1. Tagged item is removed from or placed in "Smart Cabinet"
1. "Smart Cabinet" periodically interrogates to assess inventory
1. Server/Database is updated to reflect item's disposition
1. Designated individuals are notified regarding items that need attention (cabinet and shelf location, action required)

Source: **How Stuff Works**

Smart fridge

- Recognizes what's been put in it
- Recognizes when things are removed
- Creates automatic shopping lists
- Notifies you when things are past their expiration

- Shows you the recipes that most closely match what is available

Smart groceries enhanced

- Track products through their entire lifetime.

Source: **How Stuff Works**

Some more smart applications

- “Smart” appliances:
  - Closets that advice on style depending on clothes available.
  - Ovens that know recipes to cook pre-packaged food.
- “Smart” products:
  - Clothing, appliances, CDs, etc. tagged for store returns.
- “Smart” paper:
  - Airline tickets that indicate your location in the airport.
- “Smart” currency:
  - Anti-counterfeiting and tracking.

- “Smart” people ??

RFID advantages over bar-codes

- No line of sight required for reading
- Multiple items can be read with a single scan

- Each tag can carry a lot of data (read/write)
- Individual items identified and not just the category

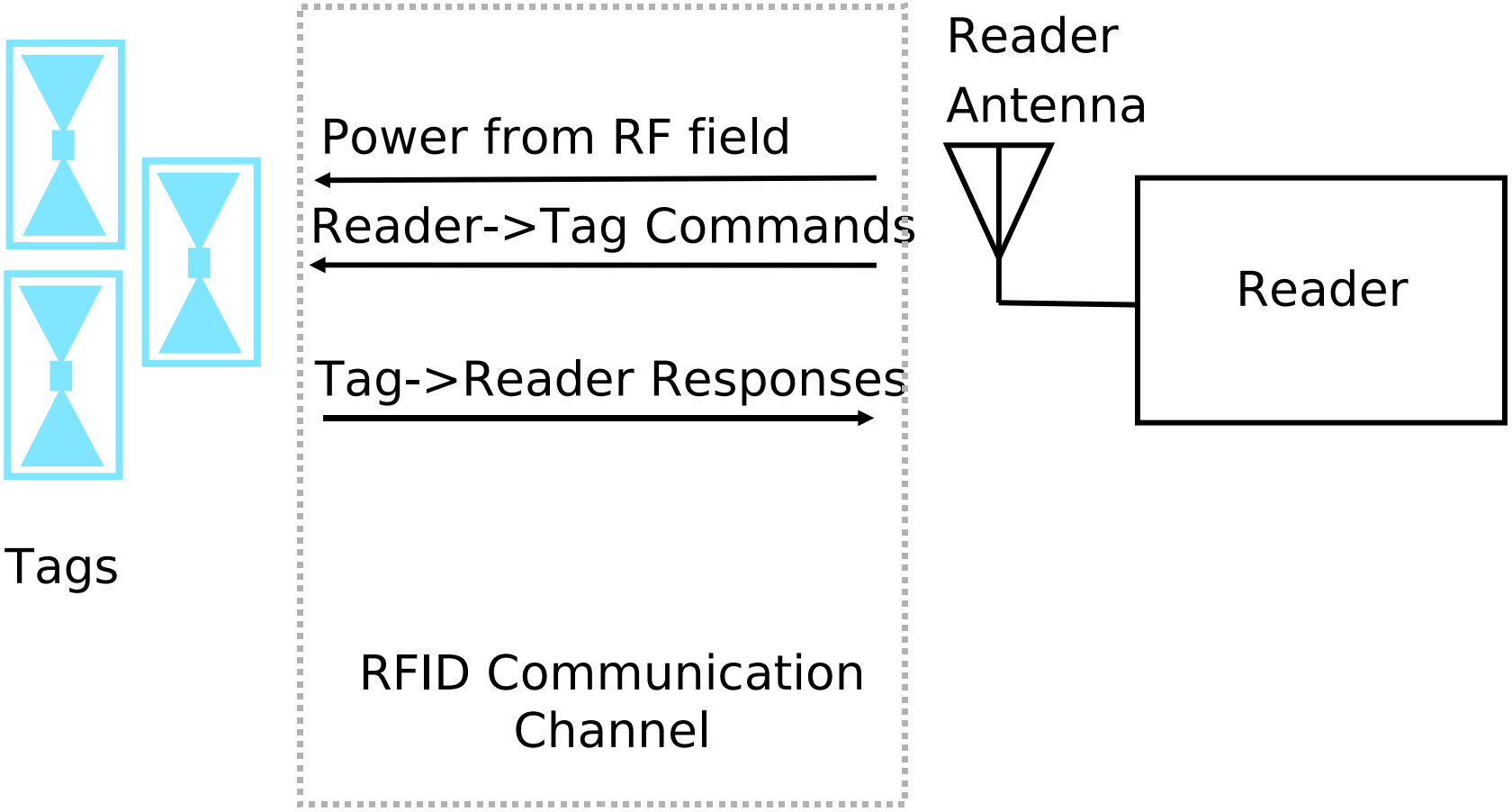
- Passive tags have a virtually unlimited lifetime
- Active tags can be read from great distances

- Can be combined with barcode technology

Outline

- Overview of RFID
  - Reader-Tag; Potential applications
- RFID Technology Internals
  - RF communications; Reader/Tag protocols
  - Middleware architecture; EPC standards
- RFID Business Aspects
- Security and Privacy
- Conclusion

RFID communications



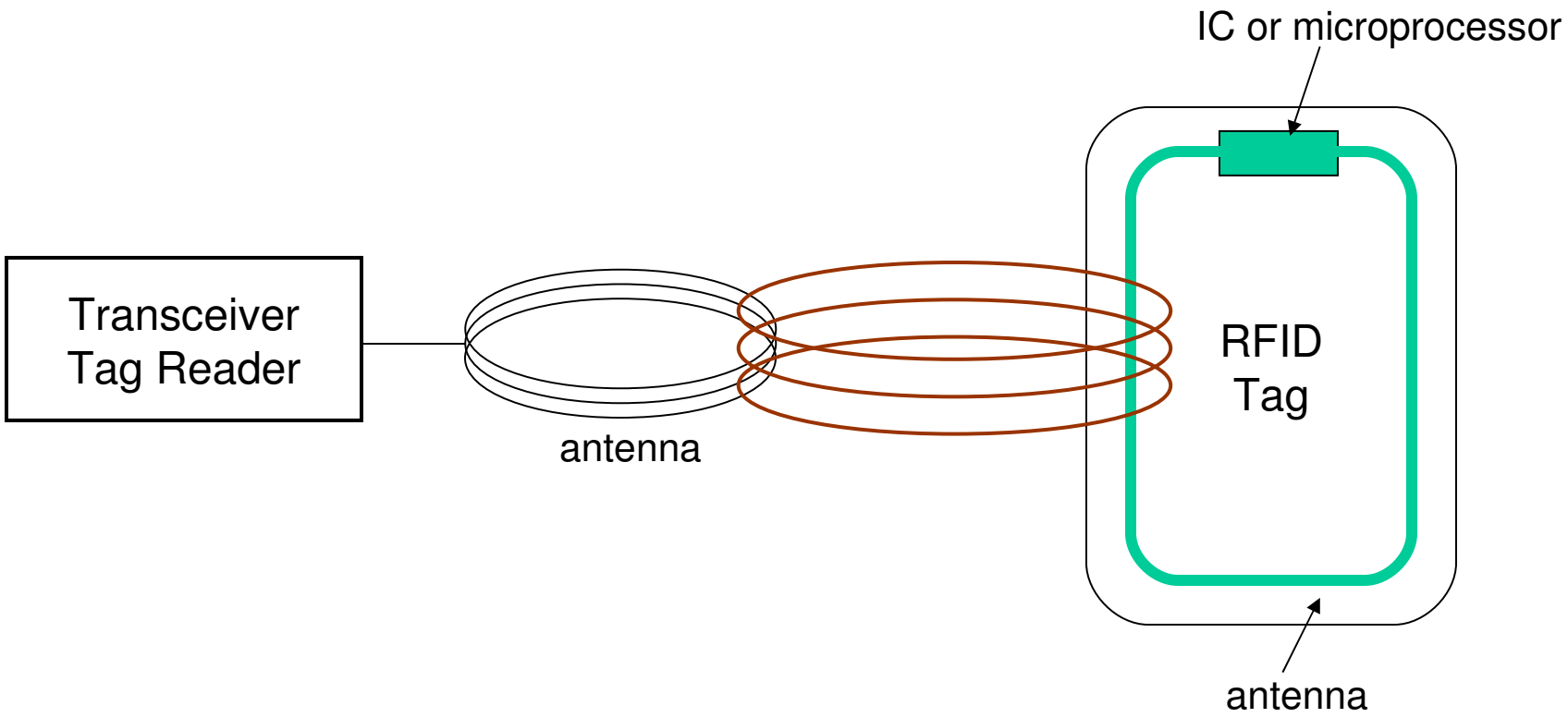
RFID communication

- Host manages Reader(s) and issues Commands

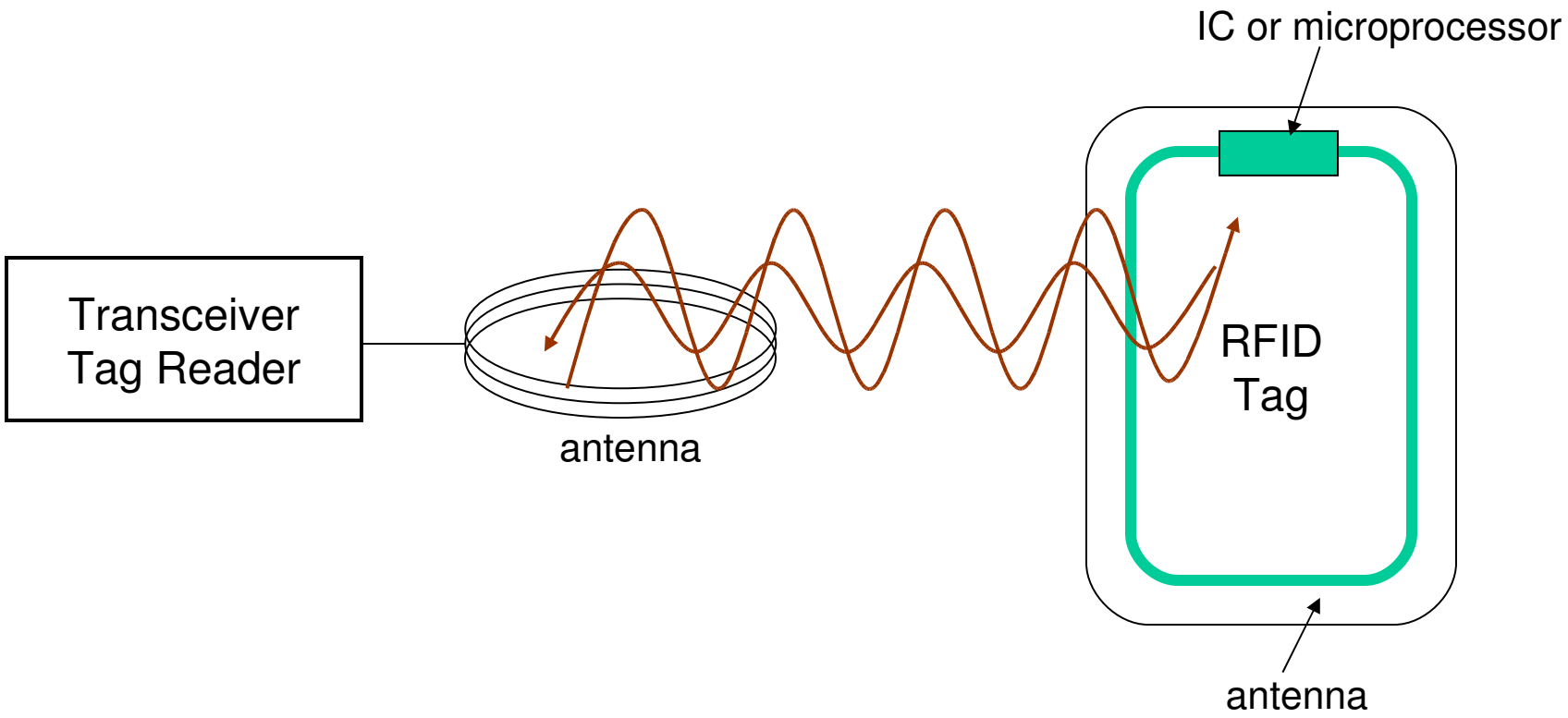
- Reader and tag communicate via RF signal
- Carrier signal generated by the reader
- Carrier signal sent out through the antennas
- Carrier signal hits tag(s)
- Tag receives and modifies carrier signal
  - "sends back" modulated signal (Passive Backscatter – also referred to as "field disturbance device")
- Antennas receive the modulated signal and send them to the Reader

- Reader decodes the data
- Results returned to the host application

Antenna fields: Inductive coupling



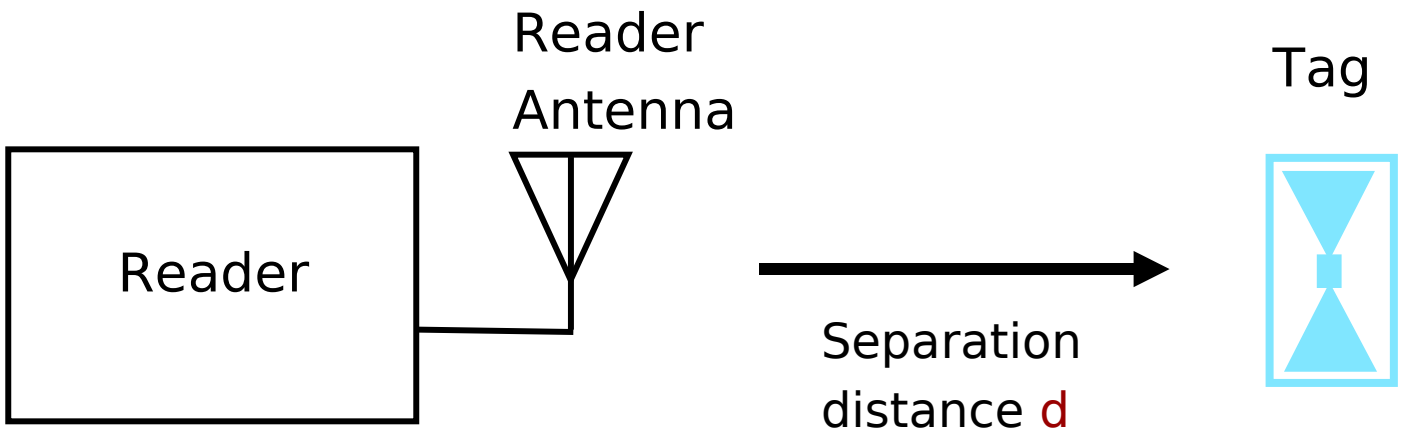
Antenna fields: Propagation coupling



Operational frequencies

Frequency Ranges	LF 125 KHz	HF 13.56 MHz	UHF 868 - 915 MHz	Microwave 2.45 GHz & 5.8 GHz
Typical Max Read Range (Passive Tags)	Shortest 1”-12”	Short 2”-24”	Medium 1’-10’	Longest 1’-15’
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive storage, E-field coupling	Active tags with integral battery or passive tags using capacitive storage, E-field coupling
Data Rate	Slower	Moderate	Fast	Faster
Ability to read near metal or wet surfaces	Better	Moderate	Poor	Worse
Applications	Access Control & Security Identifying widgets through manufacturing processes or in harsh environments Ranch animal identification Employee IDs	Library books Laundry identification Access Control Employee IDs	supply chain tracking Highway toll Tags	Highway toll Tags Identification of private vehicle fleets in/out of a yard or facility Asset tracking

Reader->Tag power transfer



Q: If a reader transmits Pr watts, how much power Pt does the tag receive at a separation distance d?

A: It depends-

UHF (915MHz) : Far field propagation : $Pt \propto 1/d^2$

HF (13.56MHz) : Inductive coupling : $Pt \propto 1/d^6$

Limiting factors for passive RFID

1. Reader transmitter power Pr (Gov't. limited)
2. Reader receiver sensitivity Sr
3. Reader antenna gain Gr (Gov't. limited)

4. Tag antenna gain Gt (Size limited)
5. Power required at tag Pt (Silicon process limited)
6. Tag modulator efficiency Et

Implications

- Since $Pt \propto 1/d^2$, doubling read range requires 4X the transmitter power.
- Larger antennas can help, but at the expense of larger physical size because $G\{t,r\} \propto Area$.
- More advanced CMOS process technology will help by reducing Pt.

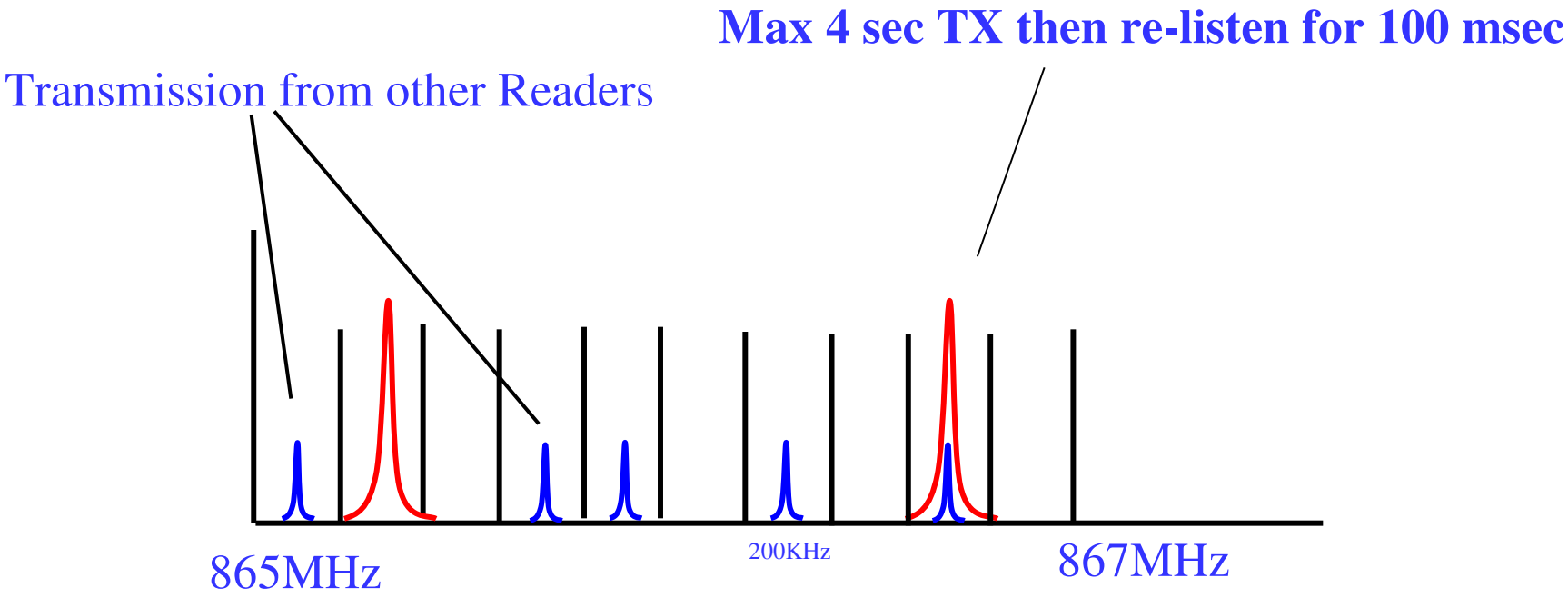
- At large distances, reader sensitivity limitations dominate.

RF effects of common materials

Material	Effect(s) on RF signal
Cardboard	Absorption (moisture) Detuning (dielectric)
Conductive liquids (shampoo)	Absorption
Plastics	Detuning (dielectric)
Metals	Reflection
Groups of cans	Complex effects (lenses, filters) Reflection
Human body / animals	Absorption, Detuning, Reflection

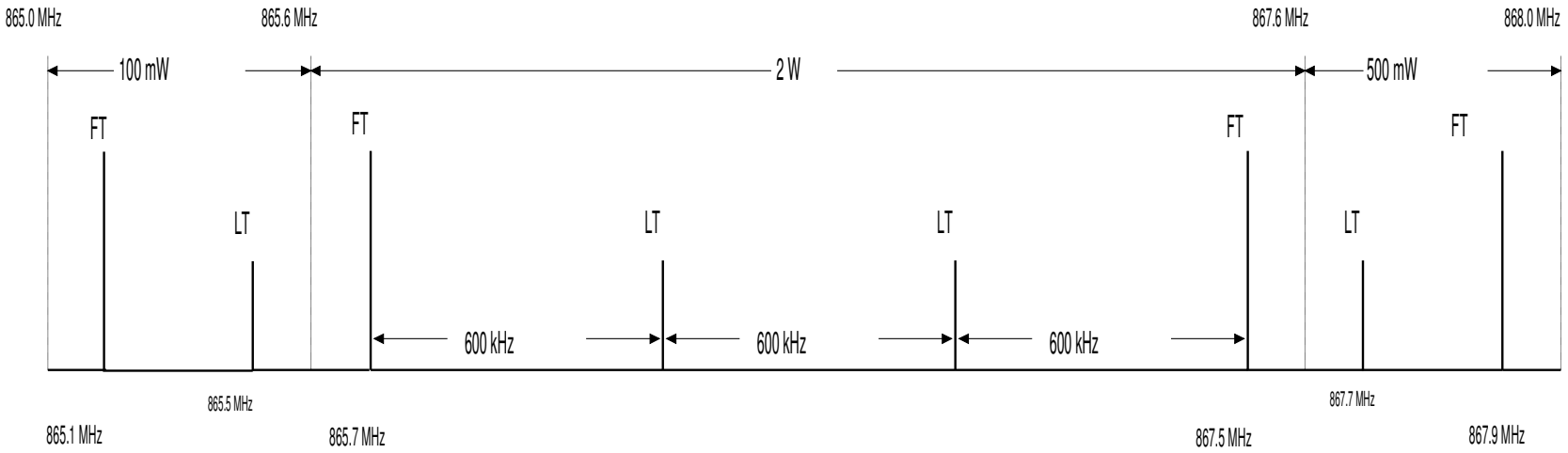
Communication protocols

- Listen before talk
- Mandatory listen time of >5 msec before each transmission



ETSI EN 302 208 standard

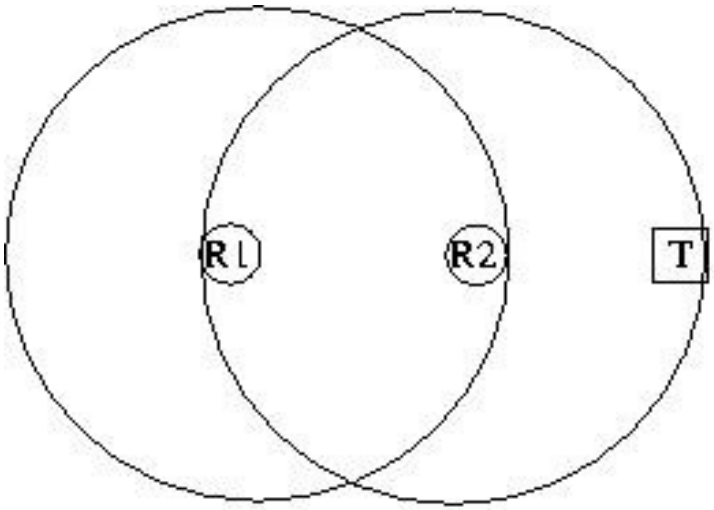
- Shared operation in band 865.0 – 868.0 MHz at transmit powers upto 2 W ERP.
  - Operation in 10 sub-bands of 200 kHz.
  - Power levels of 100 mW, 500 mW and 2 W ERP.
- Mandatory “listen before talk” and “look before leap”.



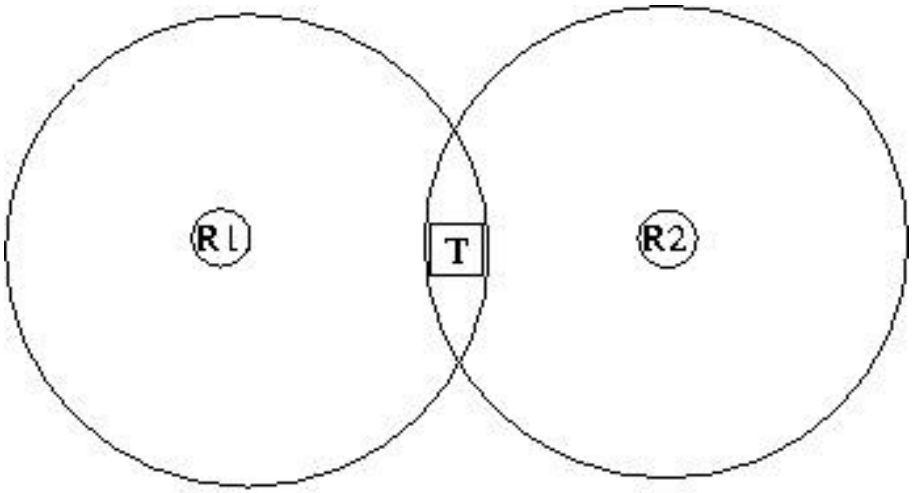
Source: **www.etsi.org**

Reader Collision Problem

- Reader-Reader Interference
- Reader-Tag Interference



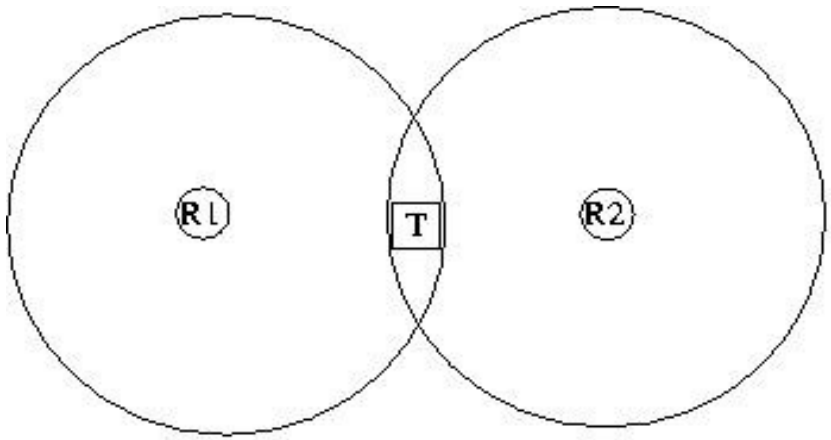
Reader to Reader Interference



Reader to Tag Interference

Reader Collision and Hidden Terminal

- The passive tags are not able to take part in the collision resolution or avoidance, as in other wireless systems
- Consider: RTS-CTS for hidden terminal problem in 802.11
  - rfid: T is not able to send a CTS in response to an RTS from R
- In case multiple readers try to read the same tag, the tag cannot respond selectively to a particular reader



R2 is a hidden terminal for R1 – T communication

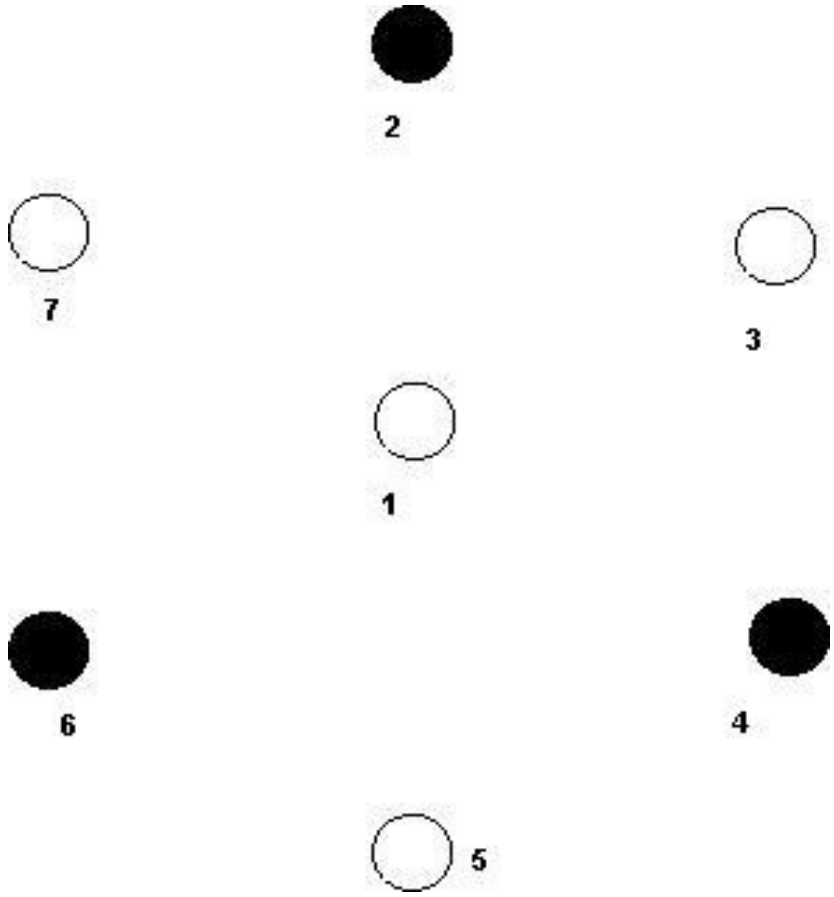
TDMA based solution

- Assign different time slots and/or frequencies to nearby readers
  - Reduces to graph coloring problem (readers form vertices)

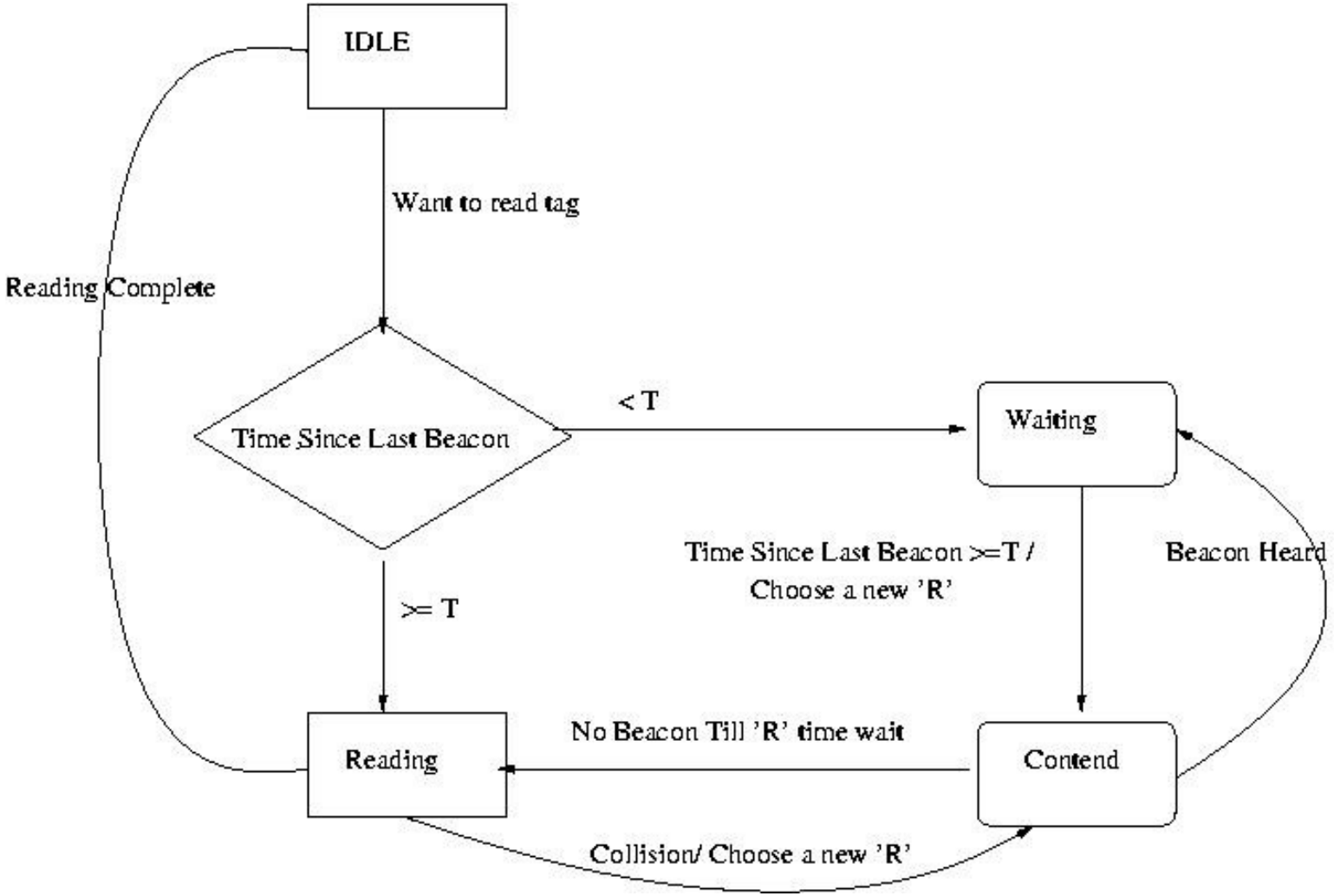
- Only reader to reader interference
  - Assign different operating frequencies
- Only multiple reader to tag interference
  - Assign different time slots for operation
- Both types of interference
  - First allot different time slots, then frequencies

Beacon based solution

- A reader while reading tag, periodically sends a beacon on the control channel
- Assumptions
  - Separate control channel between readers
  - The range in the control channel is sufficient for a reader to communicate with all the possible readers that might interfere in the data channel



Beacon based solution (contd.)



Multiple Tags

When multiple tags are in range of the reader:

- All the tags will be excited at the same time.
- Makes it very difficult to distinguish between the tags.

Collision avoidance mechanisms:

- Probabilistic:
  - Tags return at random times.
- Deterministic:
  - Reader searches for specific tags.

Tag Collision Problem

- Multiple tags simultaneously respond to query
  - Results in collision at the reader

- Several approaches
  - Tree algorithm
  - Memoryless protocol
  - Contactless protocol
  - I-code protocol

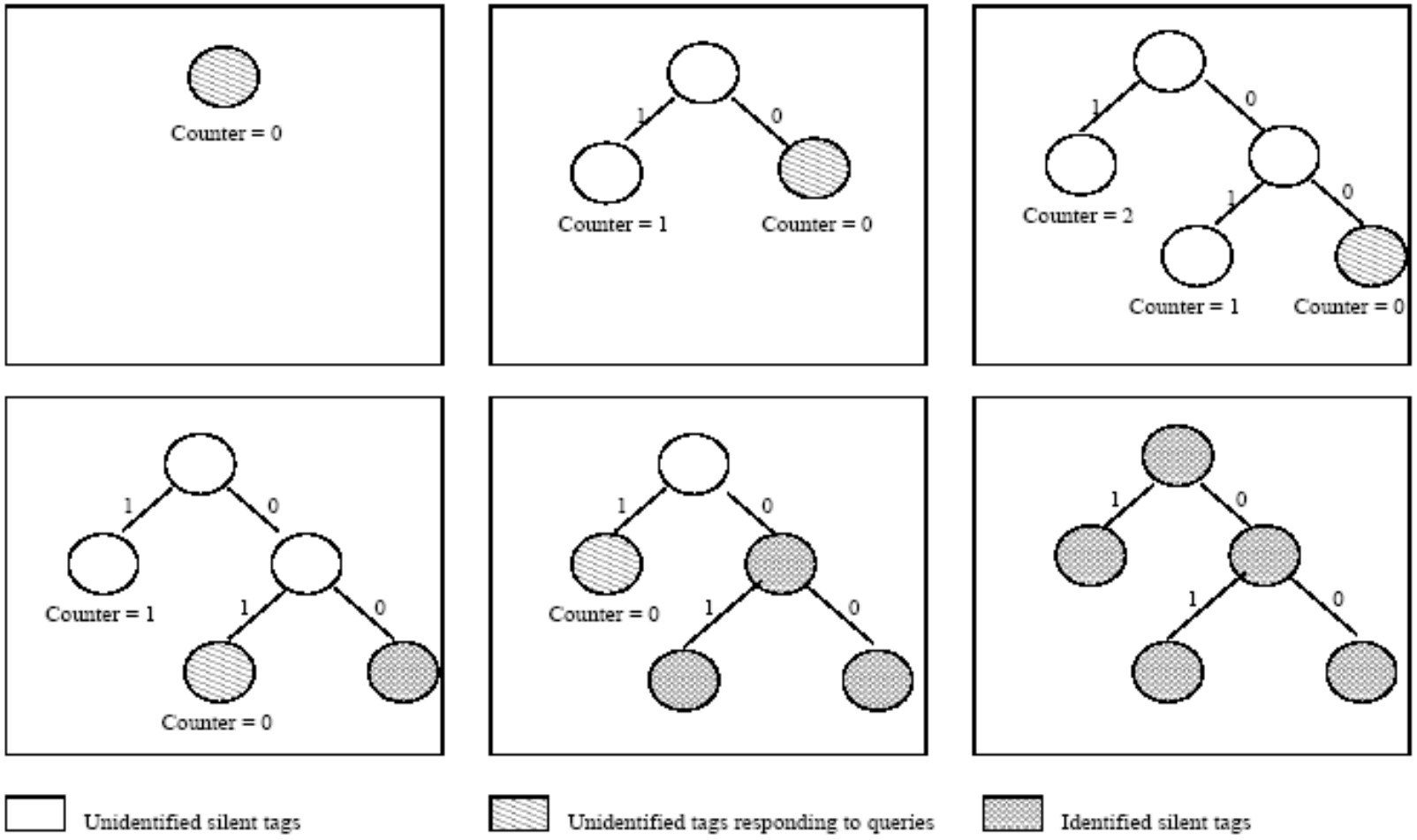
Tree Algorithm

- Reader queries for tags
- Reader informs in case of collision and tags generates 0 or 1 randomly
- If 0 then tag retransmits on next query
- If 1 then tag becomes silent and starts incrementing its counter (which is initially zero)
- Counter incremented every time collision reported and decremented every time identification reported
- Tag remains silent till its counter becomes zero

Tree Algorithm – Example

Reader informs tags in case of collision and tags generate 0 or 1

•If 0 then tag retransmits on next query, else tag becomes silent and starts a counter. Counter incremented every time collision reported and decremented otherwise.



Tree Algorithm - Complexity

- Time Complexity – $O(n)$ where n is number of tags to be identified
- Message Complexity
  - n is unknown – $\theta(nlogn)$
  - n is known - $\theta(n)$
- Overheads
  - Requires random number generator
  - Requires counter

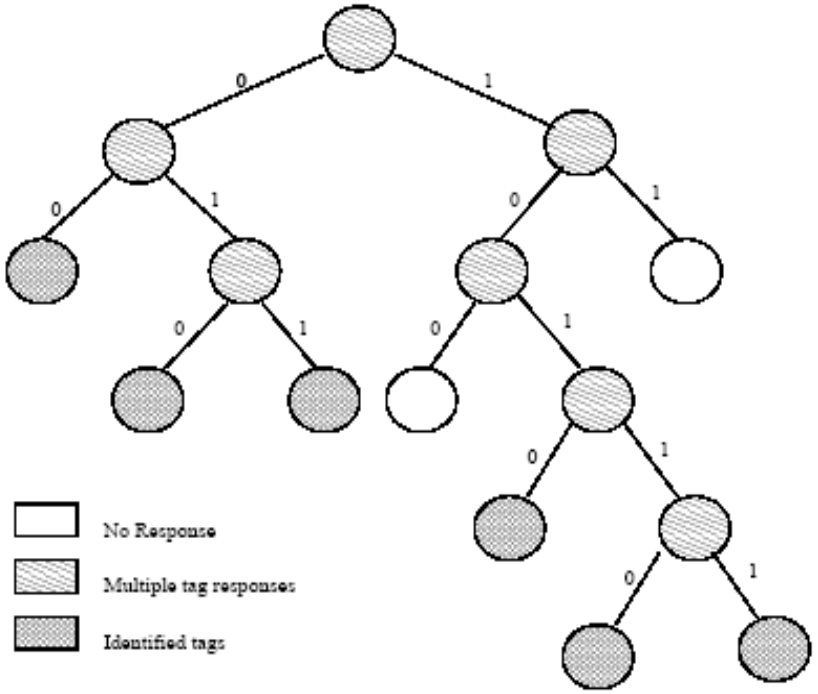
Memoryless Protocol

- Assumption: tagID stored in *k* bit binary string
- Algorithm
  - Reader queries for prefix *p*
  - In case of collision queries for *p*0 or *p*1
- Time complexity
  - Running time – *O(n)*
  - Worst Case – *n*(k + 2 – logn)*
- Message Complexity – *k*(2.21logn + 4.19)*

Memoryless Protocol – Example

- Reader queries for prefix *p*
- In case of collision, reader queries for *p*0 or *p*1
- Example: consider tags with prefixes: 00111, 01010, 01100, 10101, 10110 and 10111

Step	Query Prefix	Response
1	0	Collision
2	1	Collision
3	00	00111 (Identified)
4	01	Collision
5	10	Collision
6	11	No Response
7	010	01010 (Identified)
8	011	01100 (Identified)
9	100	No Response
10	101	Collision
11	1010	10101 (Identified)
12	1011	Collision
13	10110	10110 (Identified)
14	10111	10111 (Identified)

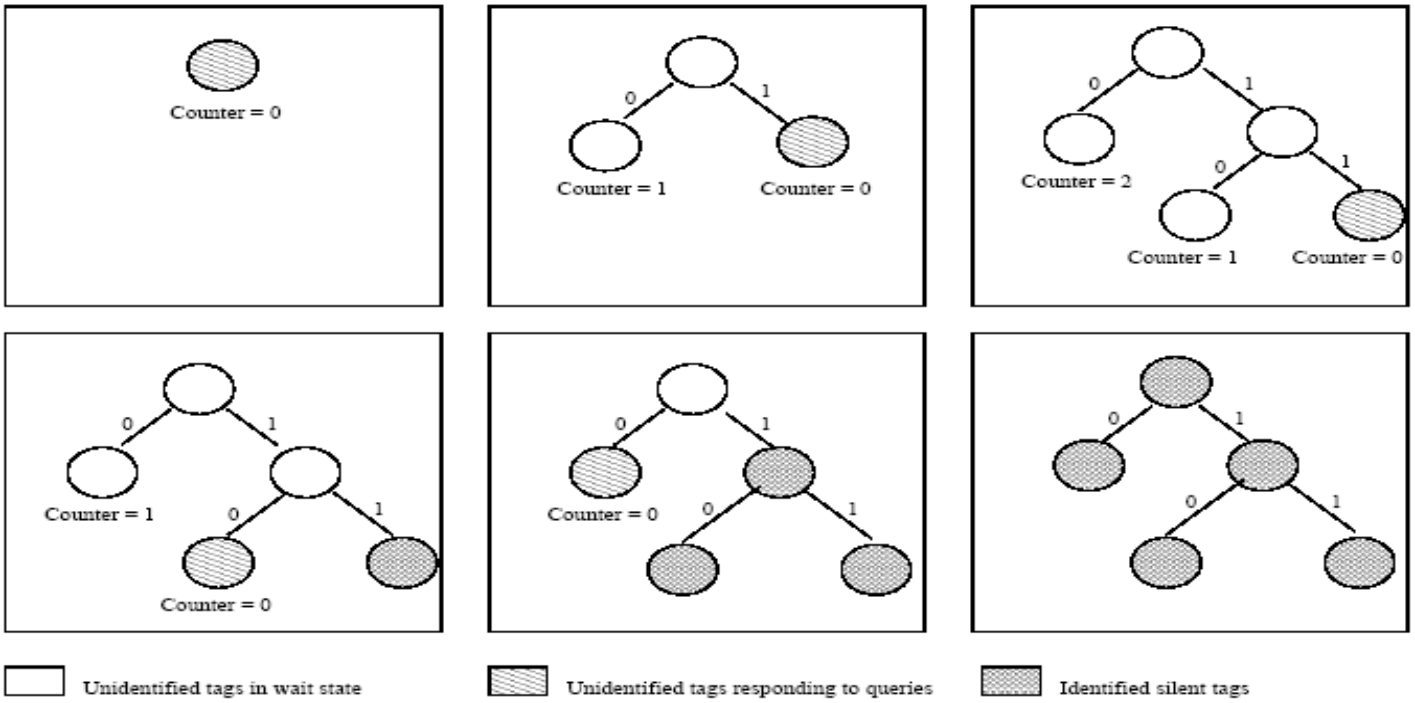


Contactless Protocol

- Assumption: tagID stored in *k* bit binary string
- Algorithm
  - Reader queries for (i)th bit
  - Reader informs in case of collision
    - Tags with (i)th bit 0 become silent and maintain counter
    - Tags with (i)th bit 1 respond to next query for (i+1)th bit
- Time complexity – $O(2^k)$
- Message complexity – $O(m(k+1))$, where m is number of tags

Contactless Protocol – Example

- Reader queries for (i)th bit
- Reader informs in case of collision
  - Tags with (i)th bit 0 become silent and maintain counter
  - Tags with (i)th bit 1 respond to next query for (i+1)th bit
- Example: tags with prefixes: 01, 10 and 11



I-Code Protocol

- Based on slotted ALOHA principle
- Algorithm
  - Reader provides time frame with *N* slots, *N* calculated for estimate *n* of tags
  - Tags randomly choose a slot and transmit their information
  - Responses possible for each slot are
    - Empty, no tag transmitted in this slot – c_0
    - Single response, identifying the tag – c_1
    - Multiple responses, collision – c_k

I-Code Protocol

- New estimate for n : lower bound

$$\varepsilon_{lb}(N, c_0, c_1, c_k) = c_1 + 2c_k$$

N slots	1	4	8	16	31	64	128	256
n_low	-	-	-	1	10	17	51	112
n_high	-	-	-	9	27	56	129	∞

- Using estimate n, N calculated
- N becomes constant after some time
- Using this N calculate number of read cycles s to identify tags with a given level of accuracy α

- Time complexity – $t_0*(s+p)$
  - t_0 is time for one read cycle
  - p number of read cycles for estimating N
- Message complexity – $n*(s+p)$

Outline

- Overview of RFID
  - Reader-Tag; Potential applications
- RFID Technology Internals
  - RF communications; Reader/Tag protocols
  - Middleware architecture; EPC standards
- RFID Business Aspects
- Security and Privacy
- Conclusion

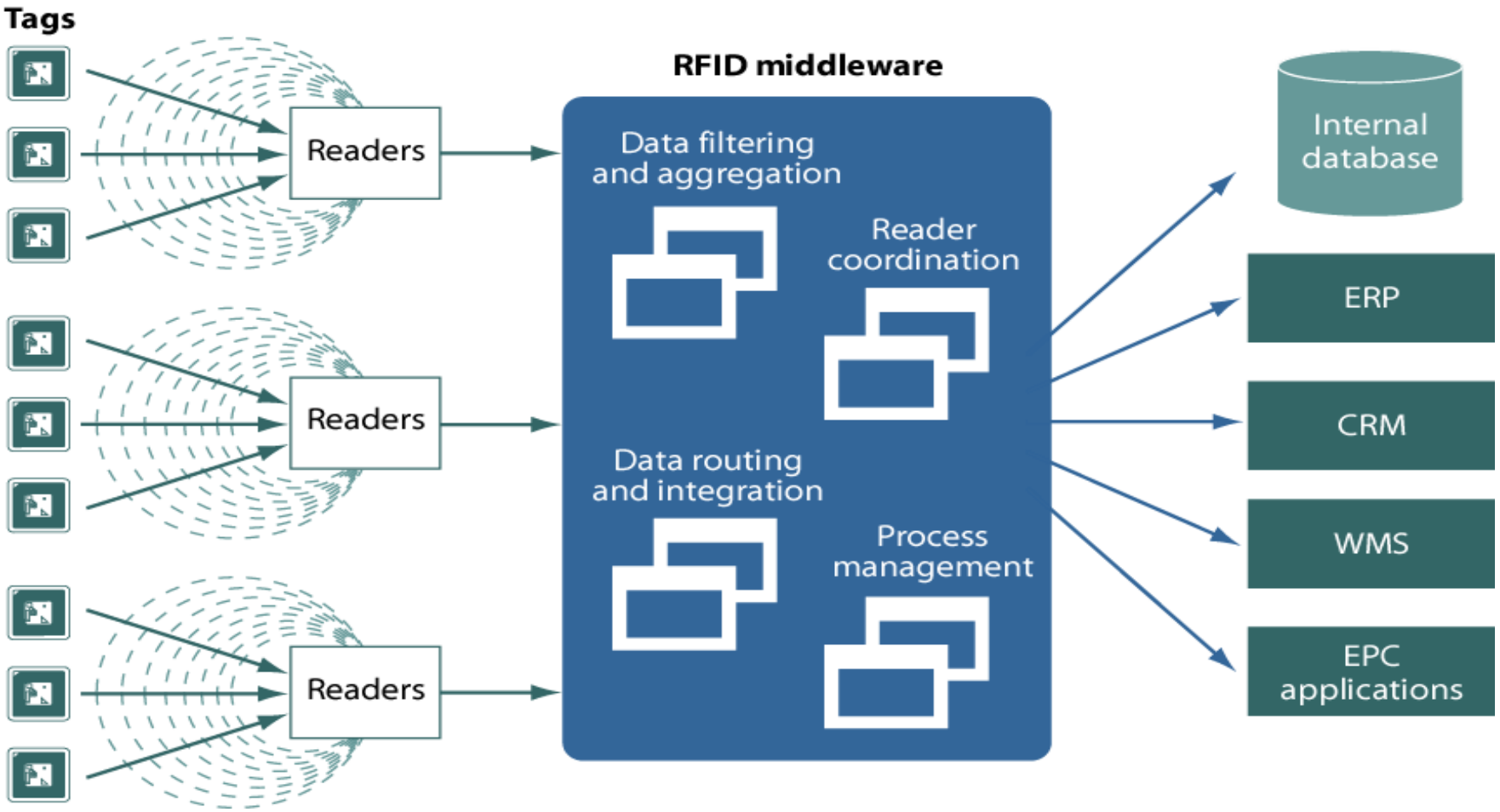
How much data?

Consider a supermarket chain implementing RFID:

- 12 bytes EPC + Reader ID + Time = 18 bytes per tag
- Average number of tags in a neighborhood store = 700,000
- Data generated per second = 12.6 GB
- Data generated per day = 544 TB
- Assuming 50 stores in the chain,
  - data generated per day = 2720 TB

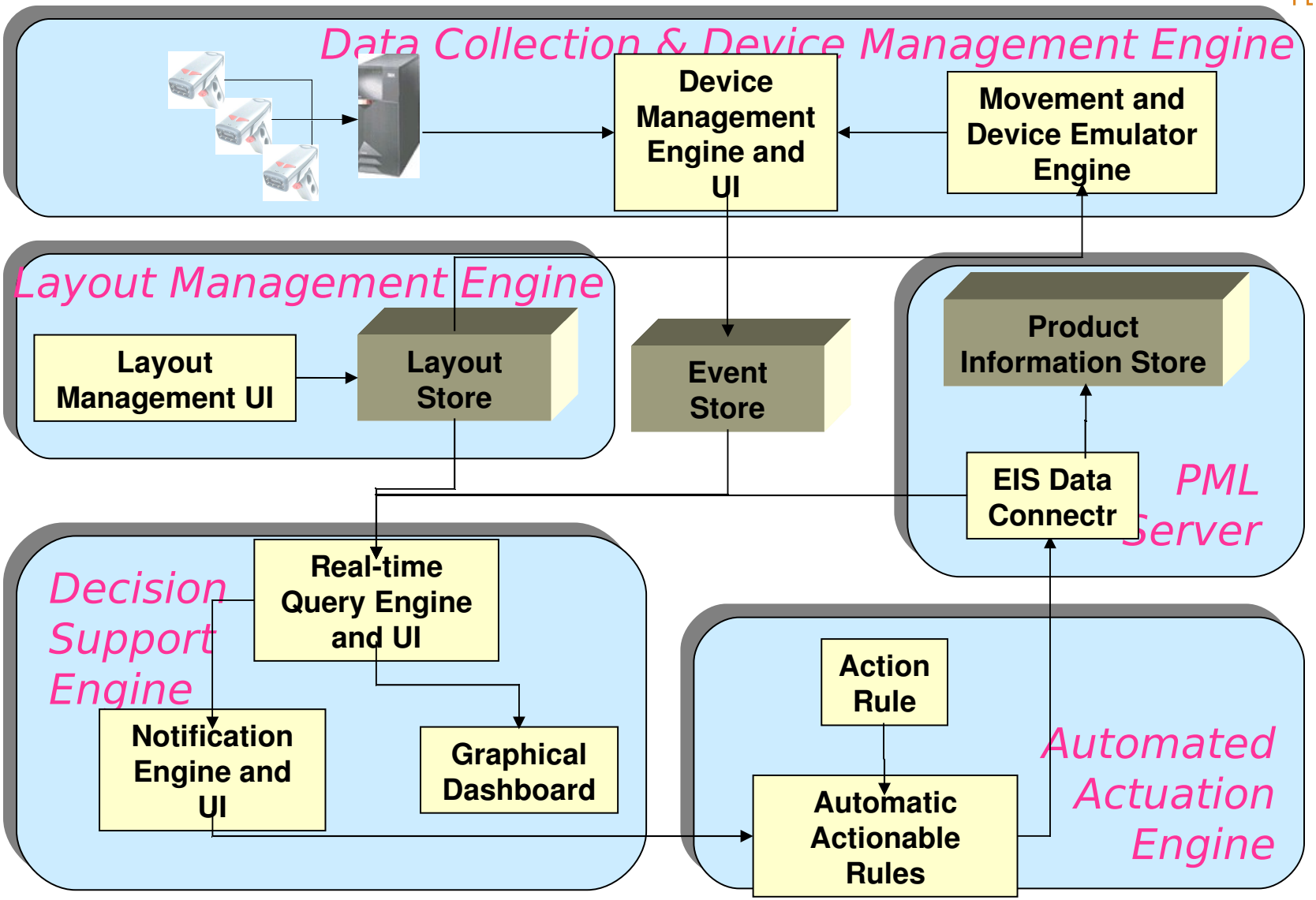
- Stanford Linear Accelerator Center generates 500 TB

RFID middleware



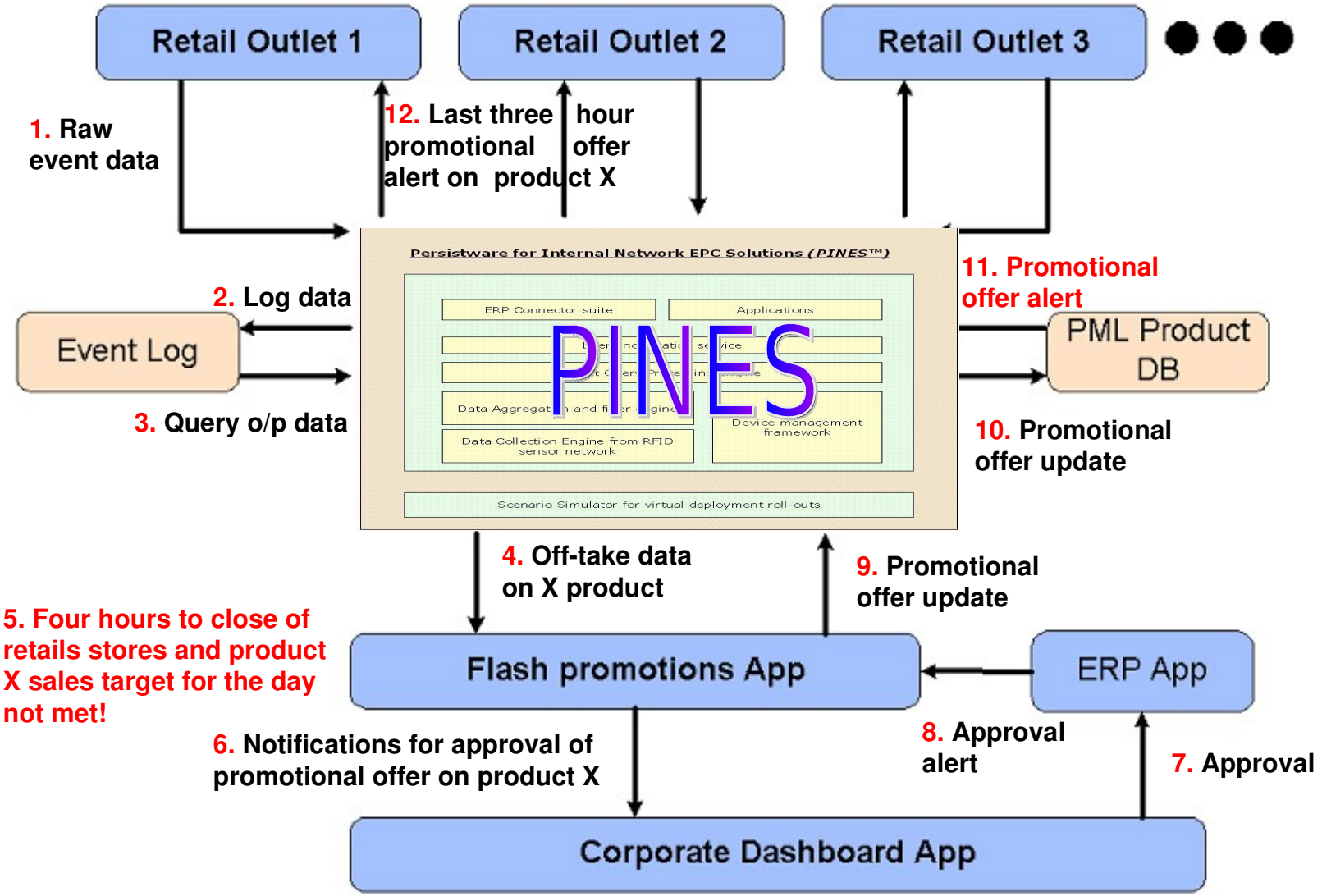
Source: **Forrester Research: RFID Middleware**

Middleware framework: PINES™



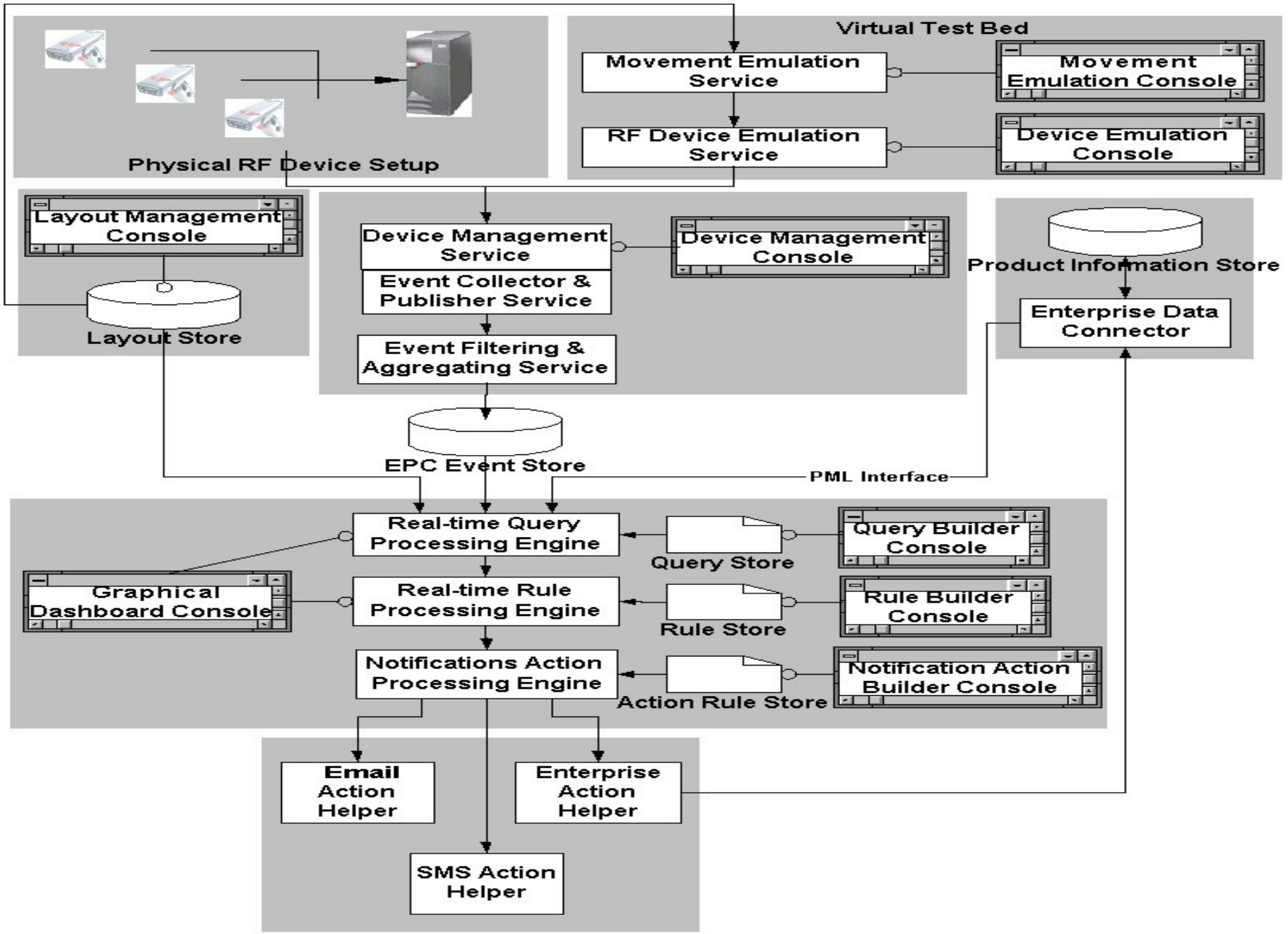
Source: **Persistent Systems**

Retail case study: Enabling real-time decisions



Source: **Persistent Systems**

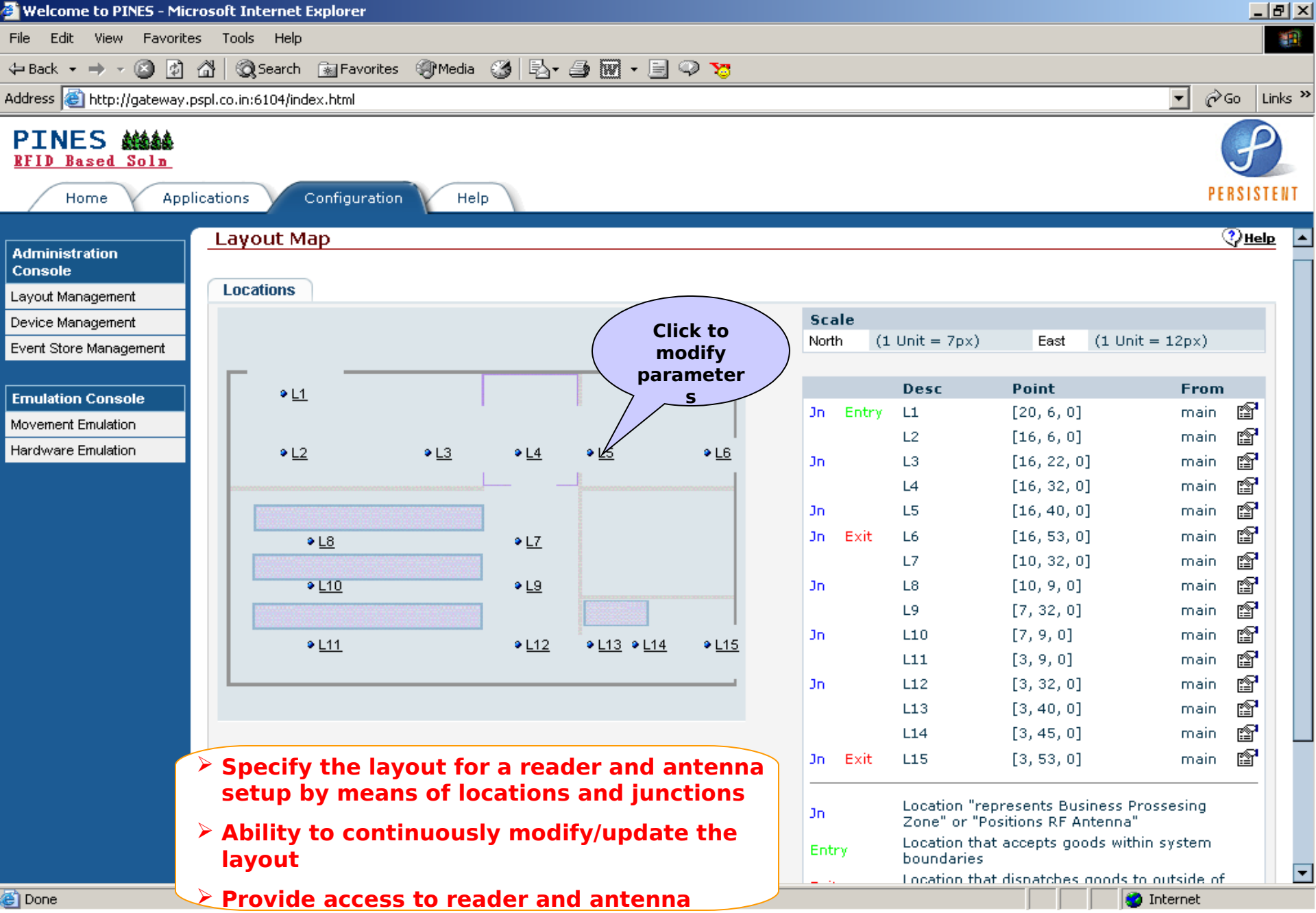
PINES™ Architecture Overview



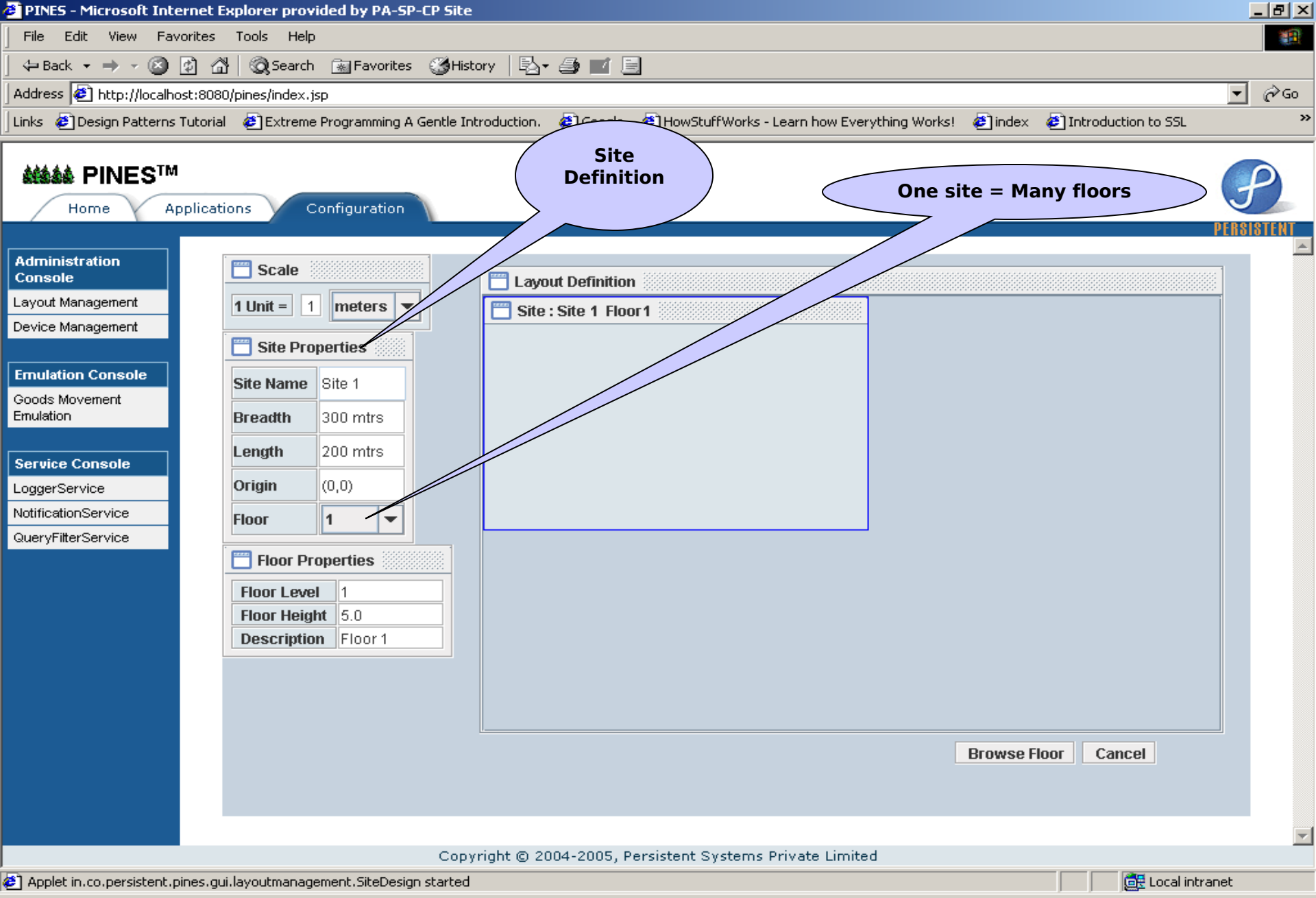
Layout Management Framework

Site Layout Configuration and Location Management

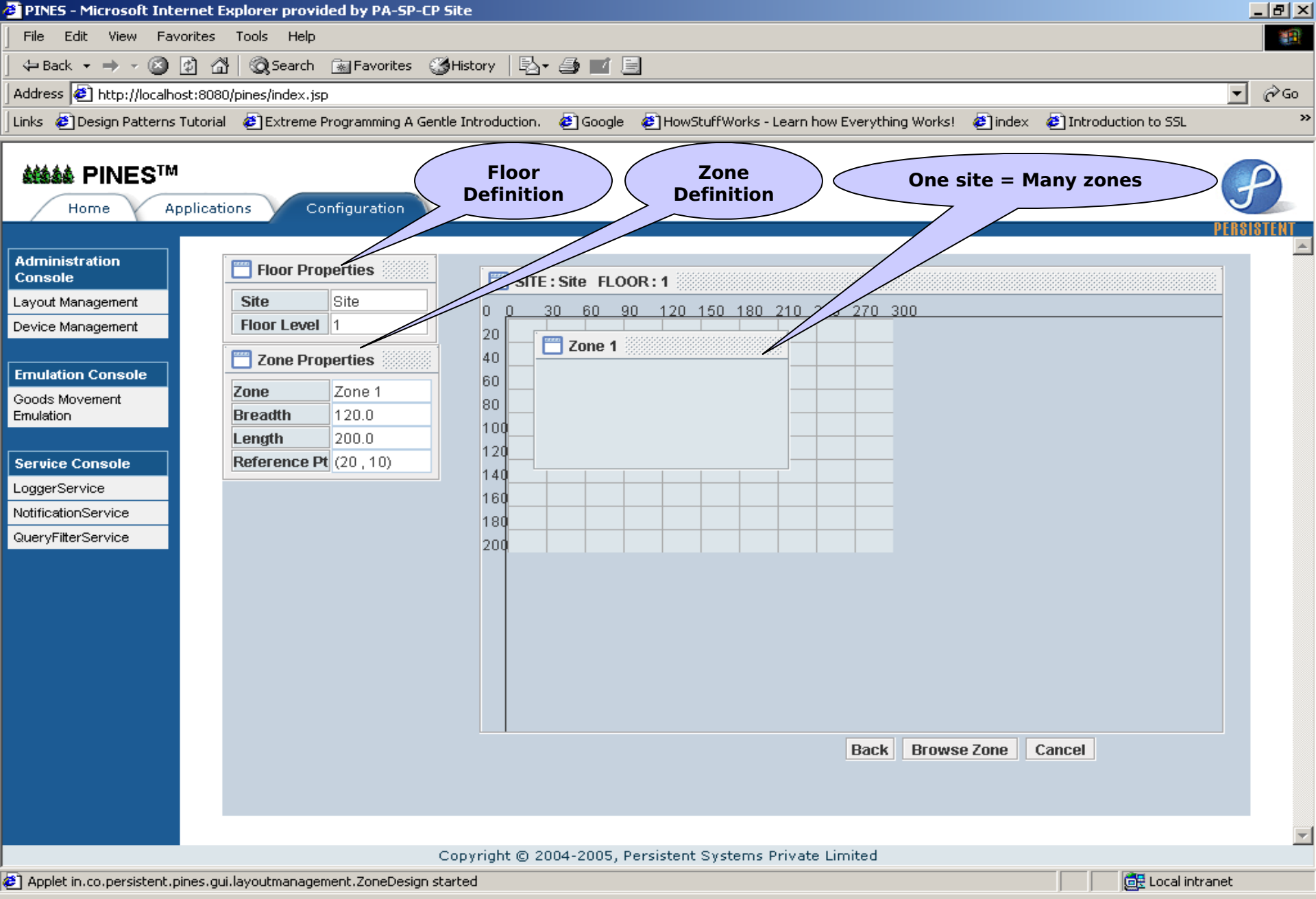
Source: **Persistent Systems**



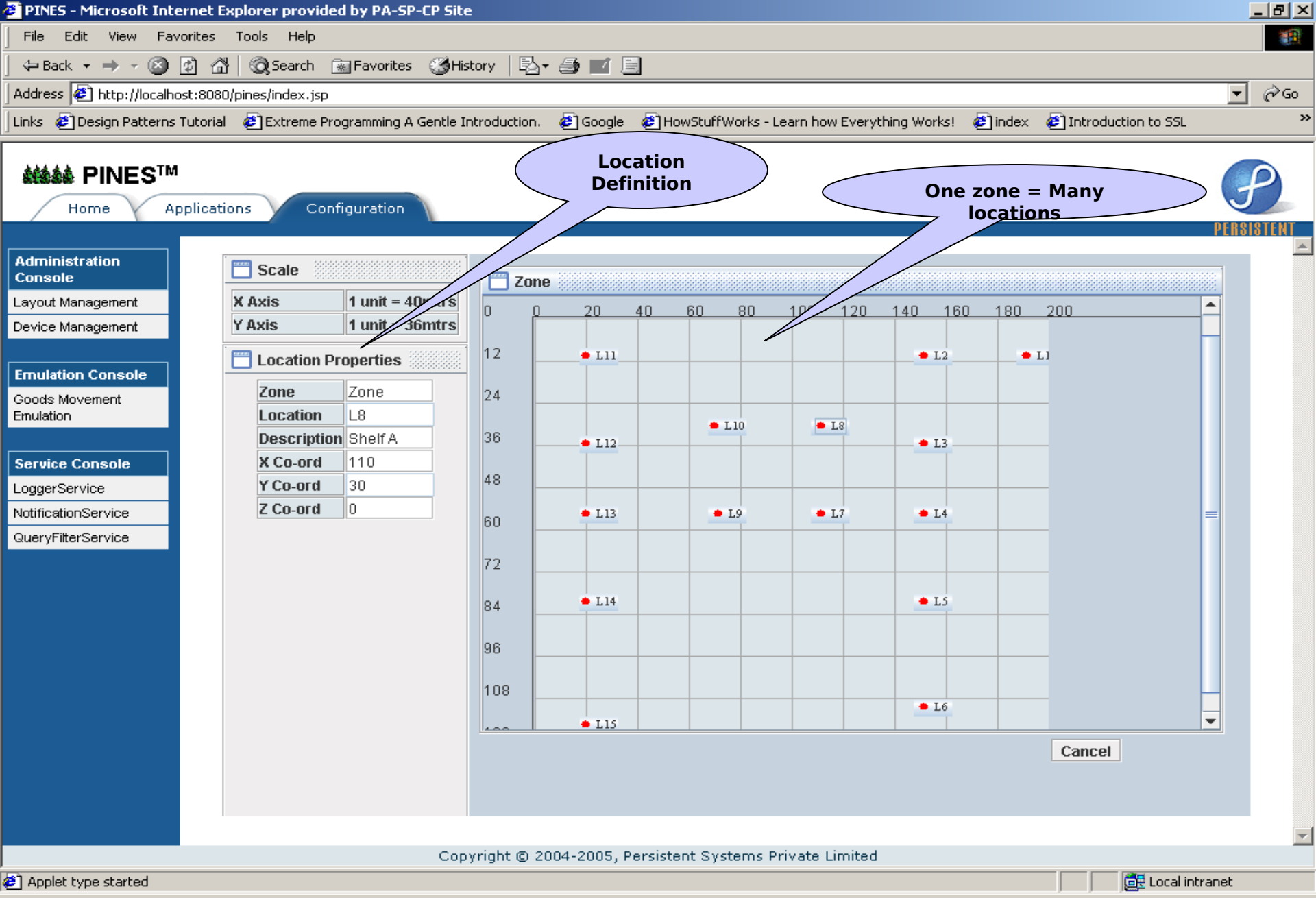
Source: **Persistent Systems**



Source: **Persistent Systems**



Source: **Persistent Systems**

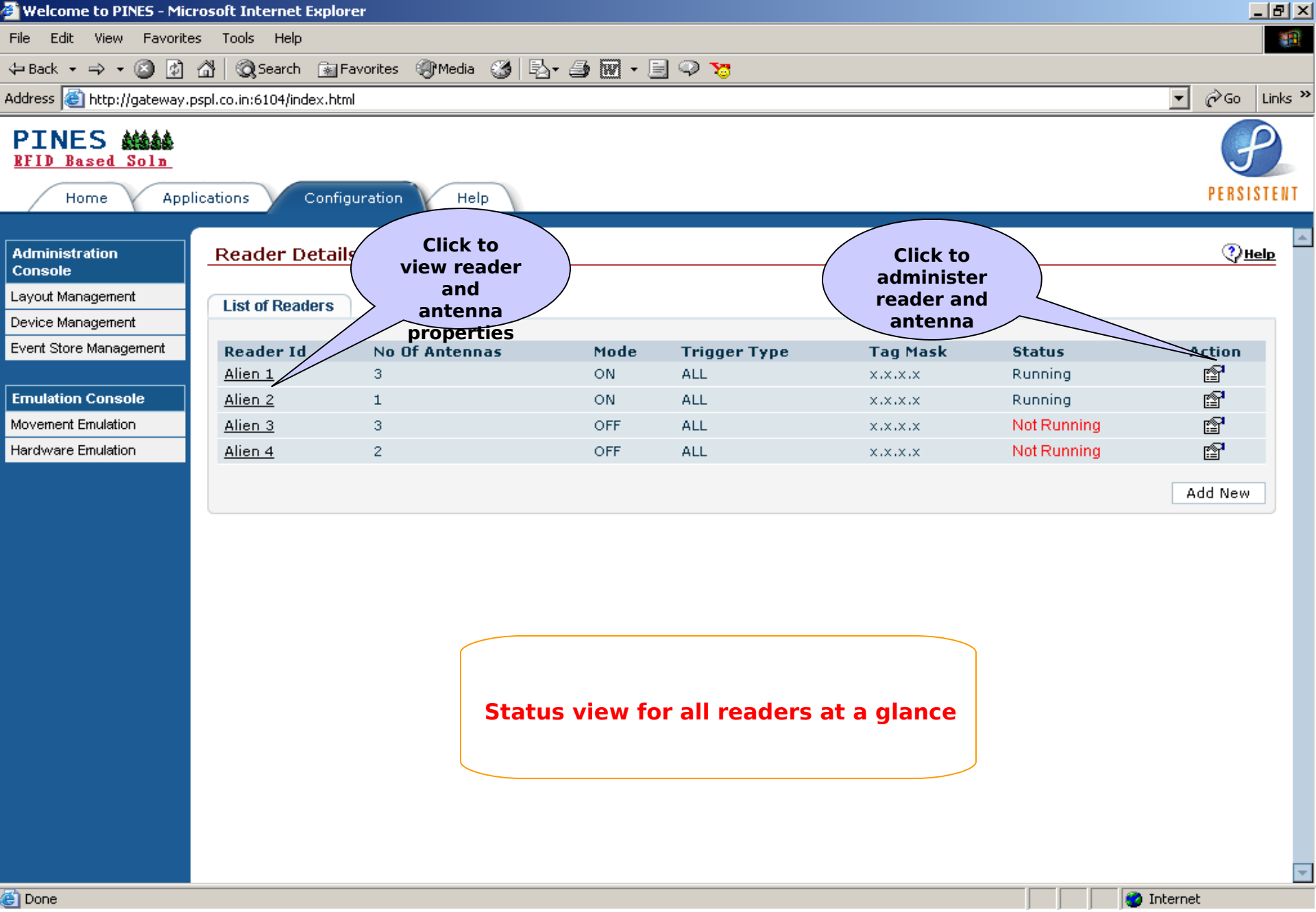


Source: **Persistent Systems**

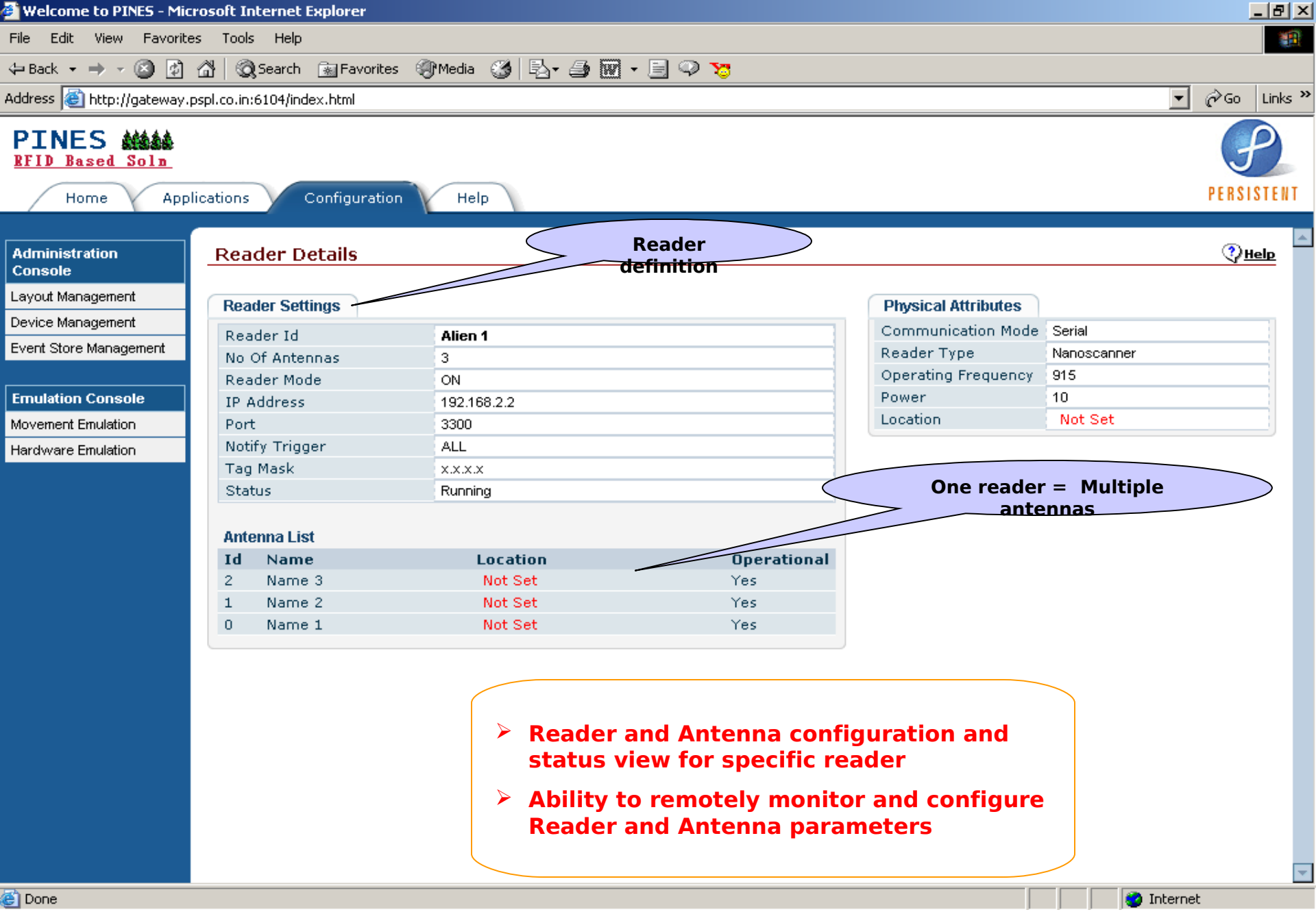
Device Management Framework

Remote monitoring and configuration of RF Sensor network elements – Readers and Antennas

Source: **Persistent Systems**



Source: **Persistent Systems**

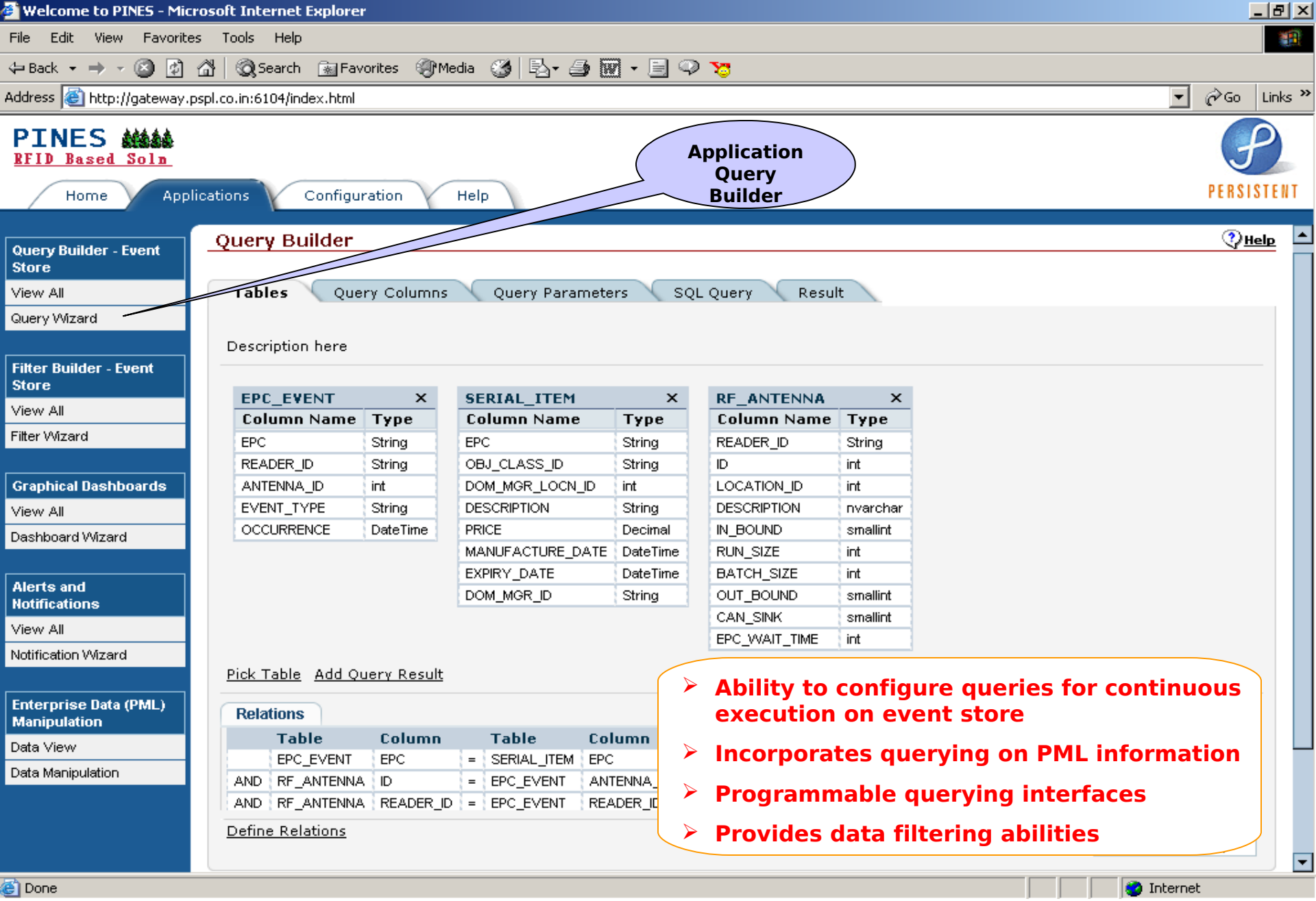


Source: **Persistent Systems**

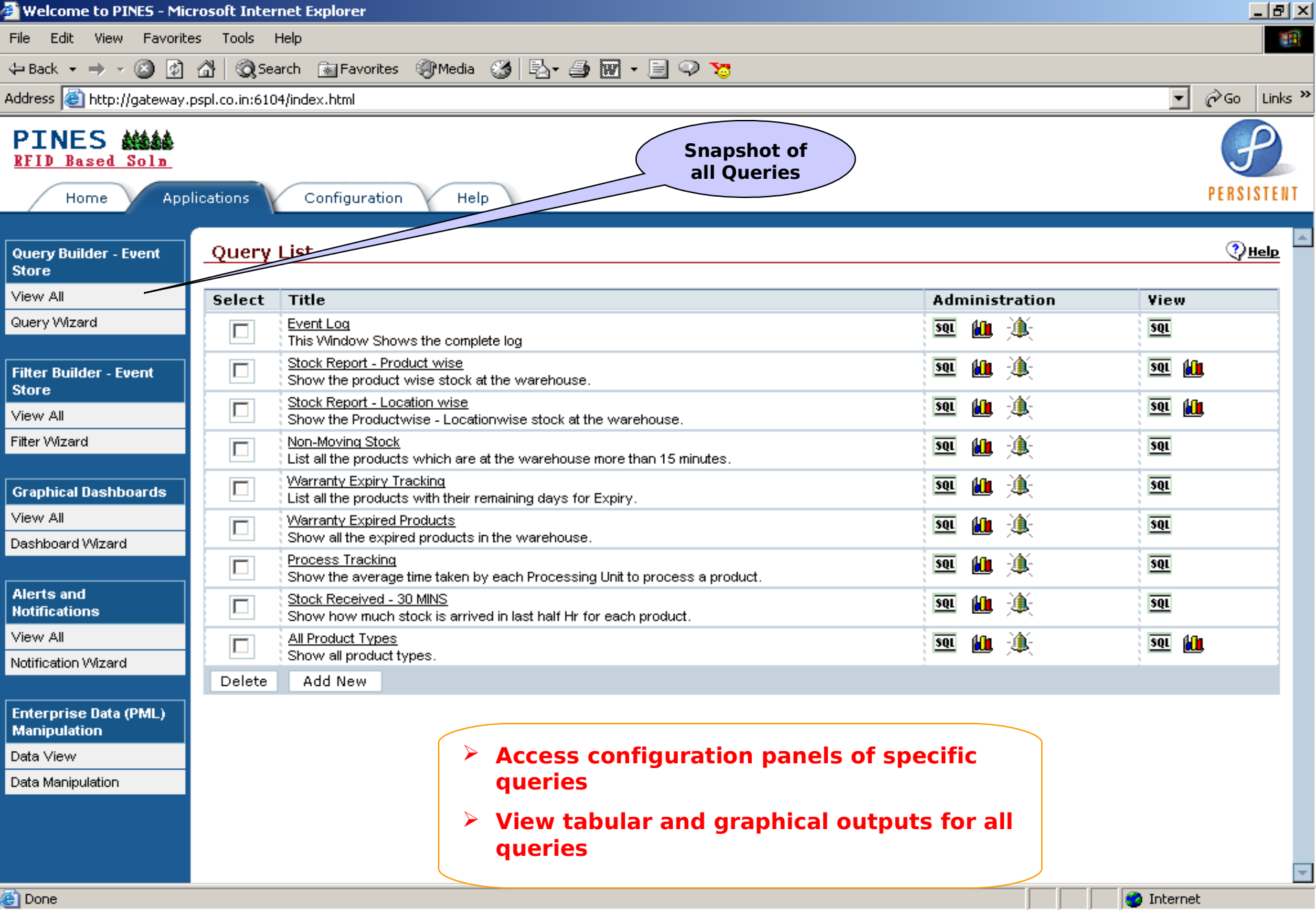
Sophisticated Query Processing

Stream based event store for incessant, high performance querying

Source: **Persistent Systems**



Source: **Persistent Systems**

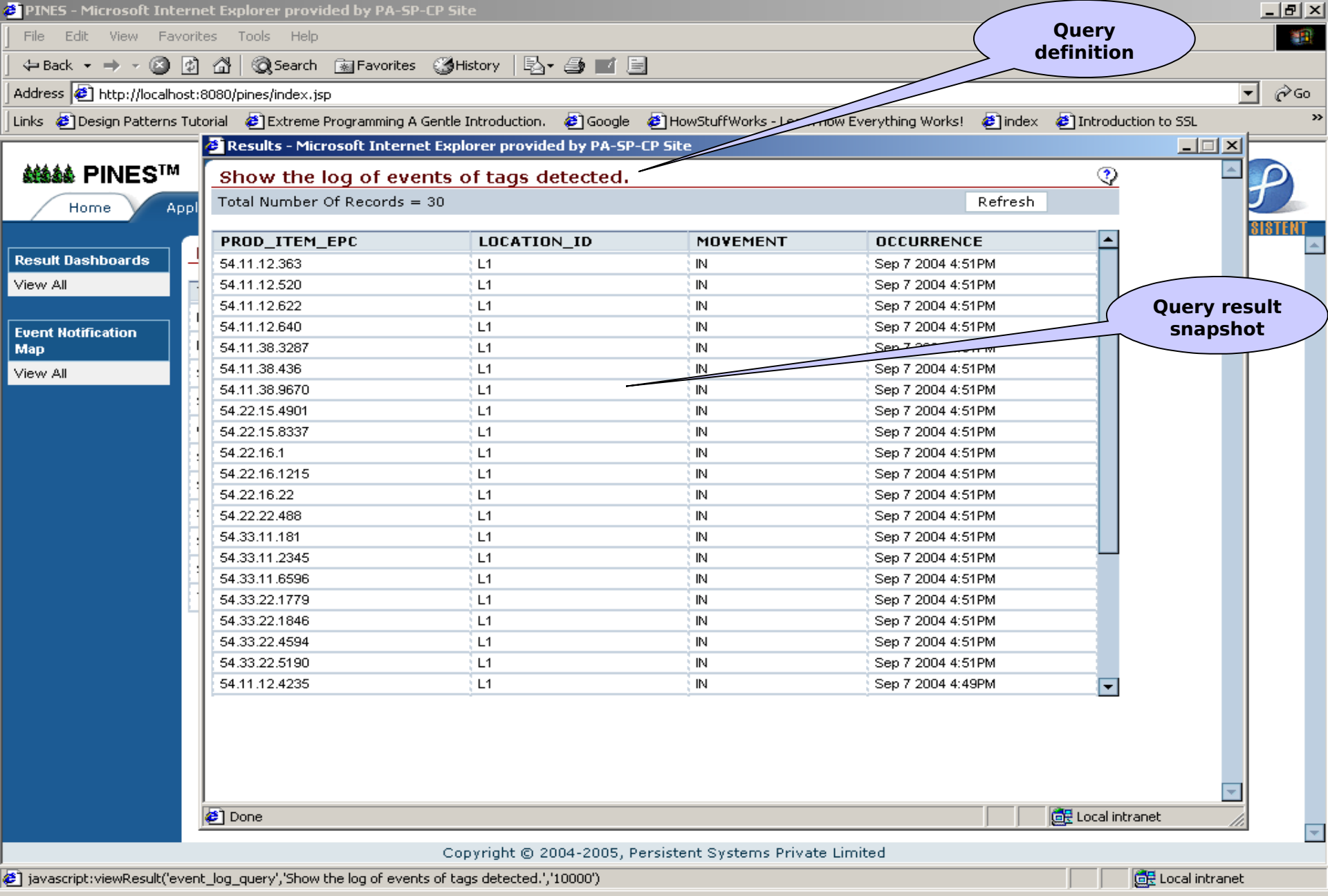


Source: **Persistent Systems**

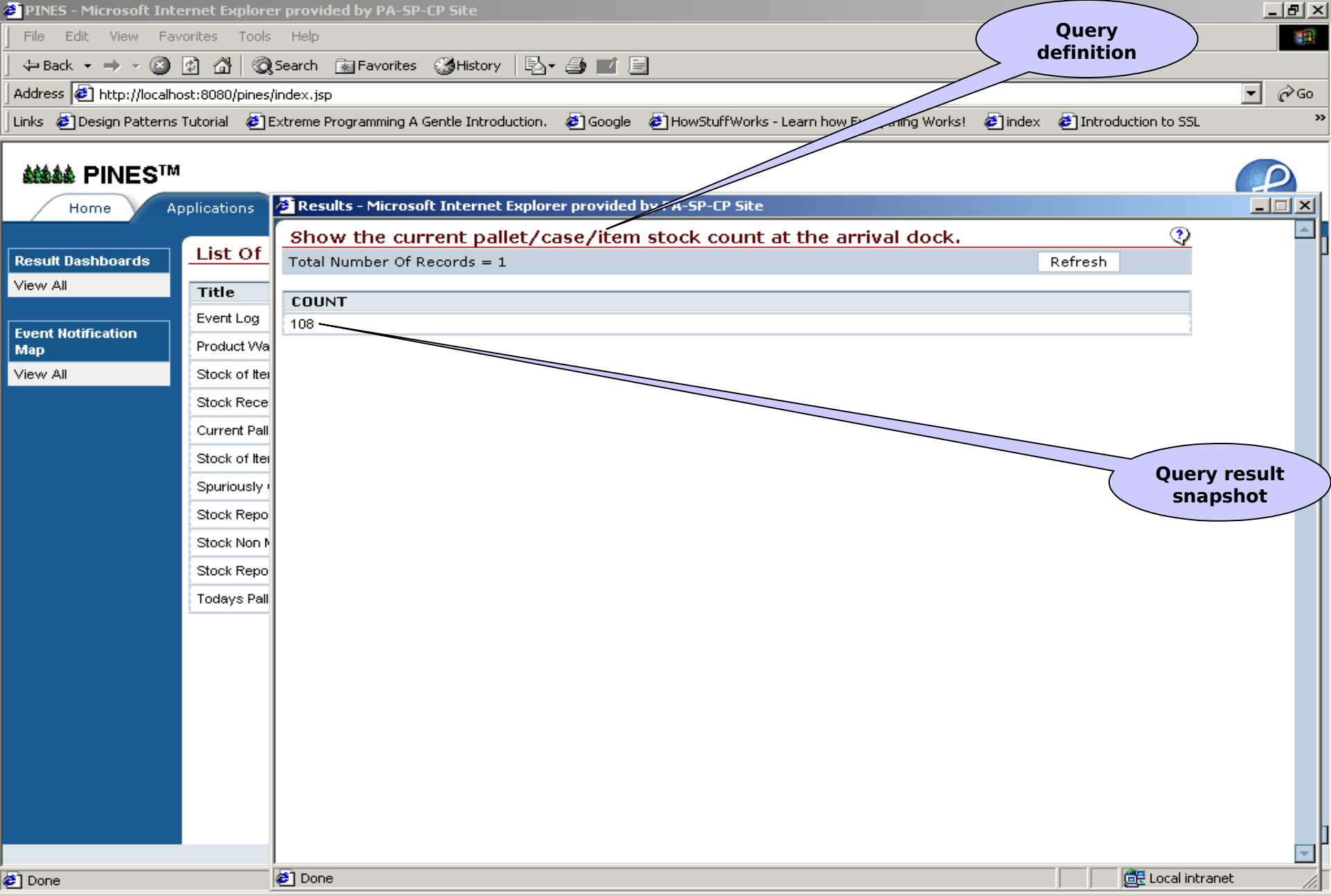
Dashboards

Corporate dashboards for enhanced decision making

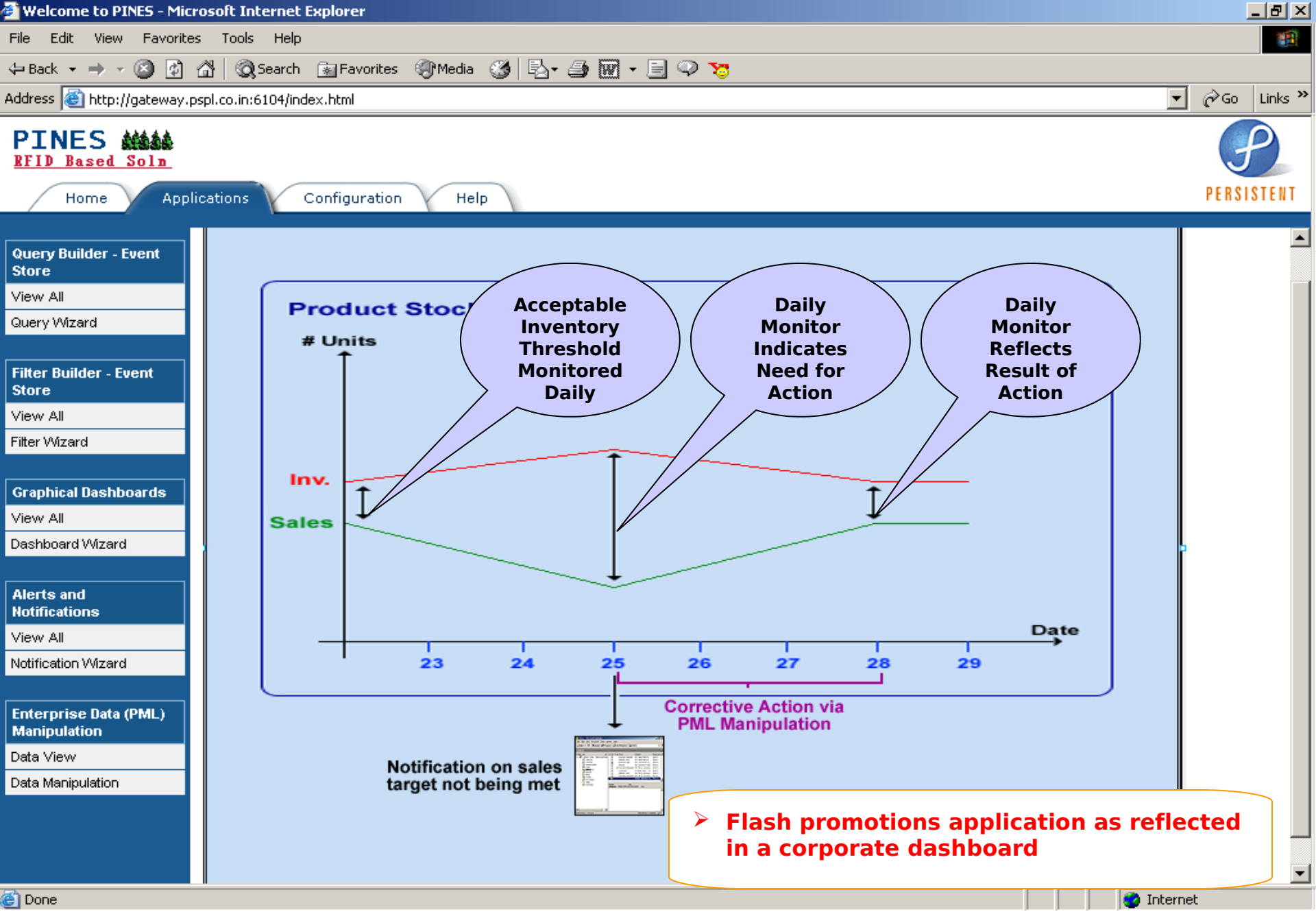
Source: **Persistent Systems**



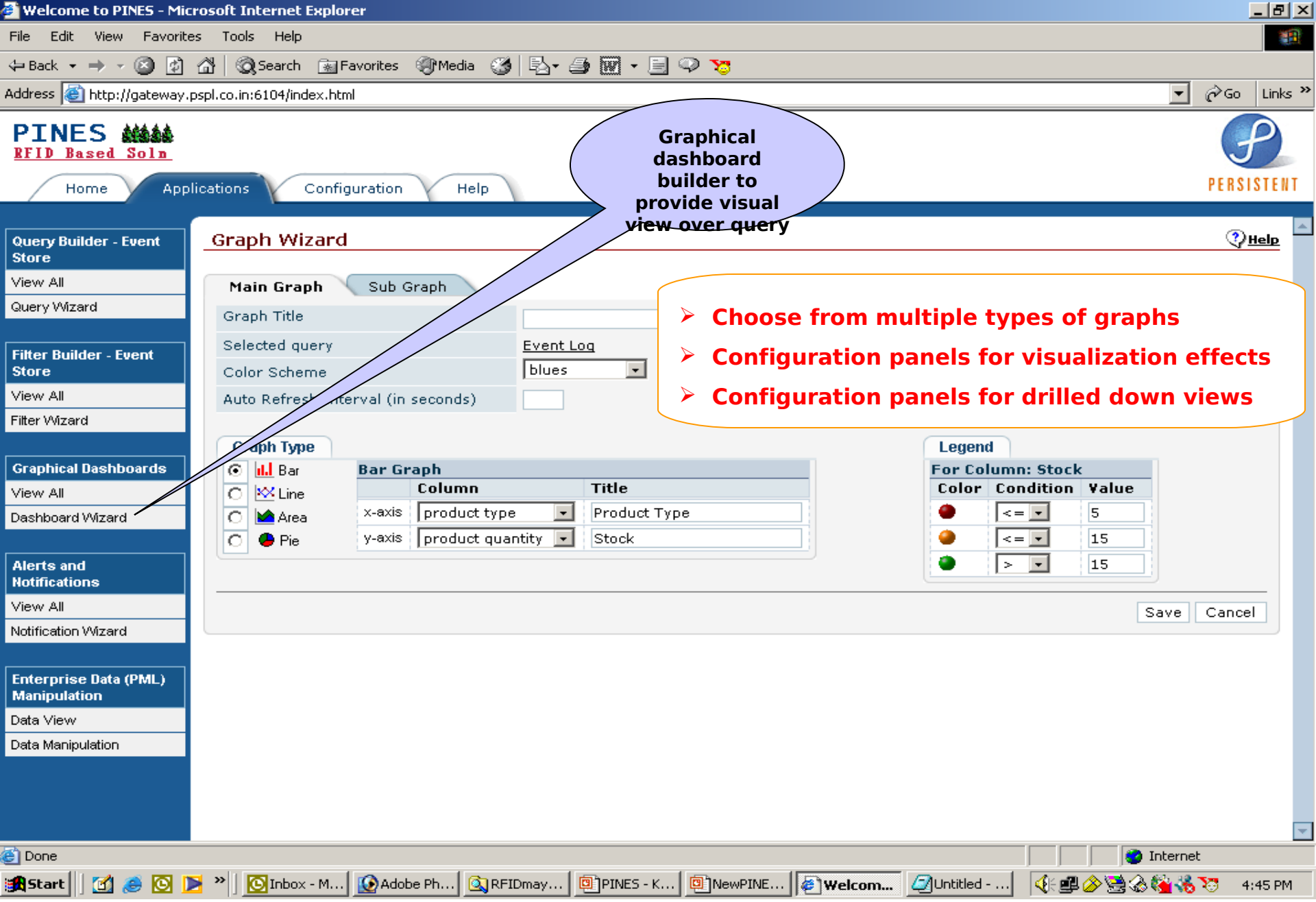
Source: **Persistent Systems**



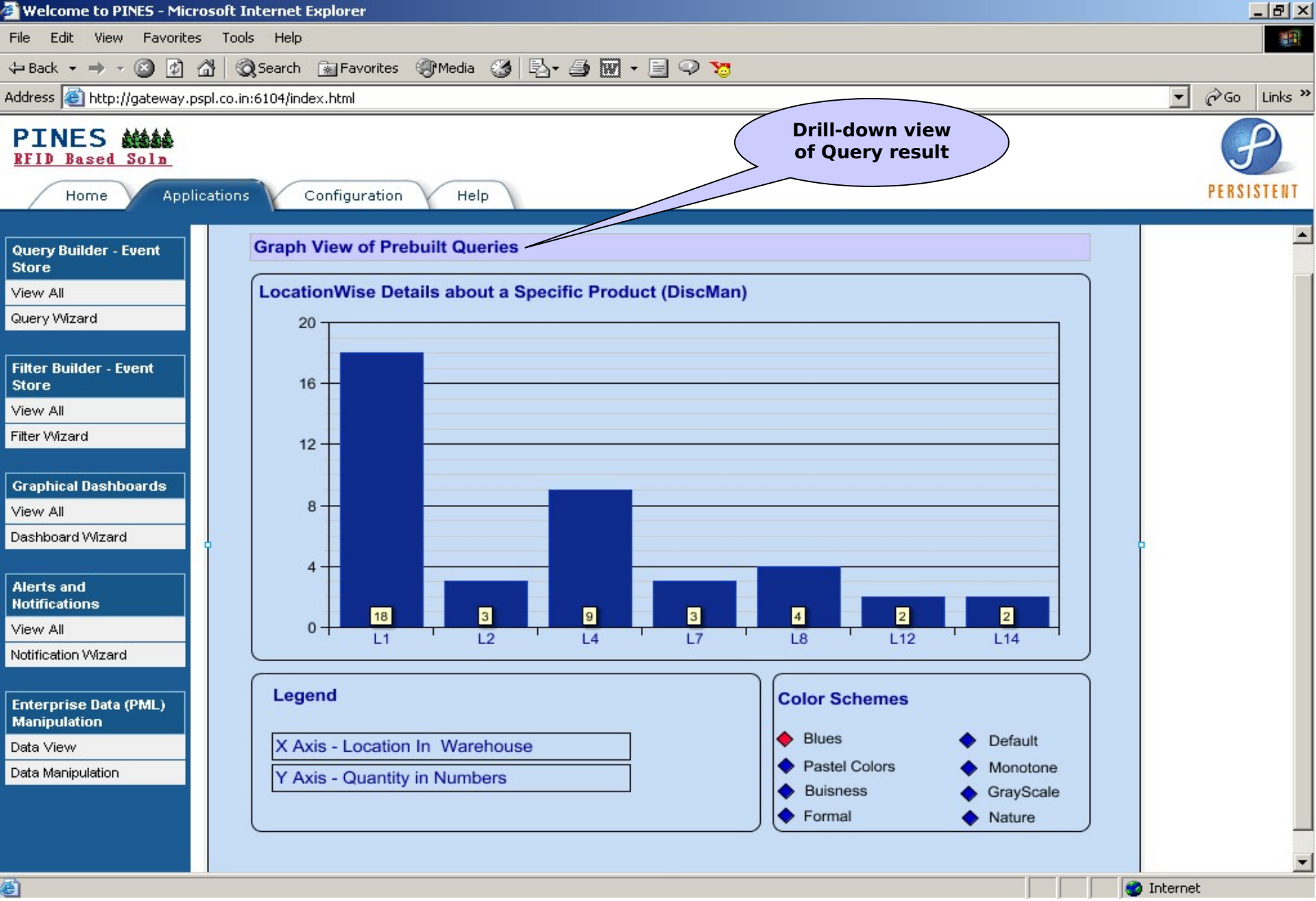
Source: **Persistent Systems**



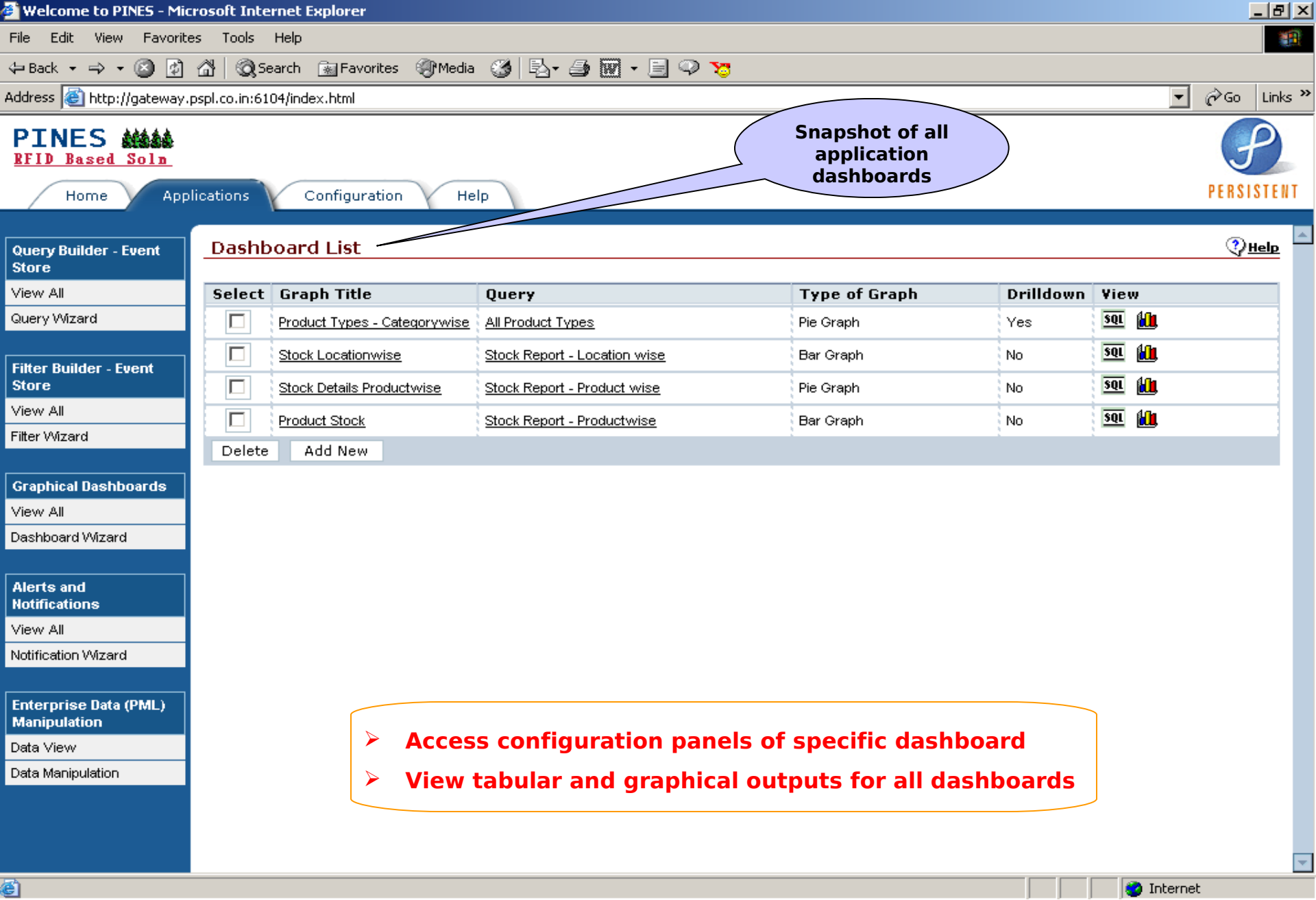
Source: **Persistent Systems**



Source: **Persistent Systems**



Source: **Persistent Systems**

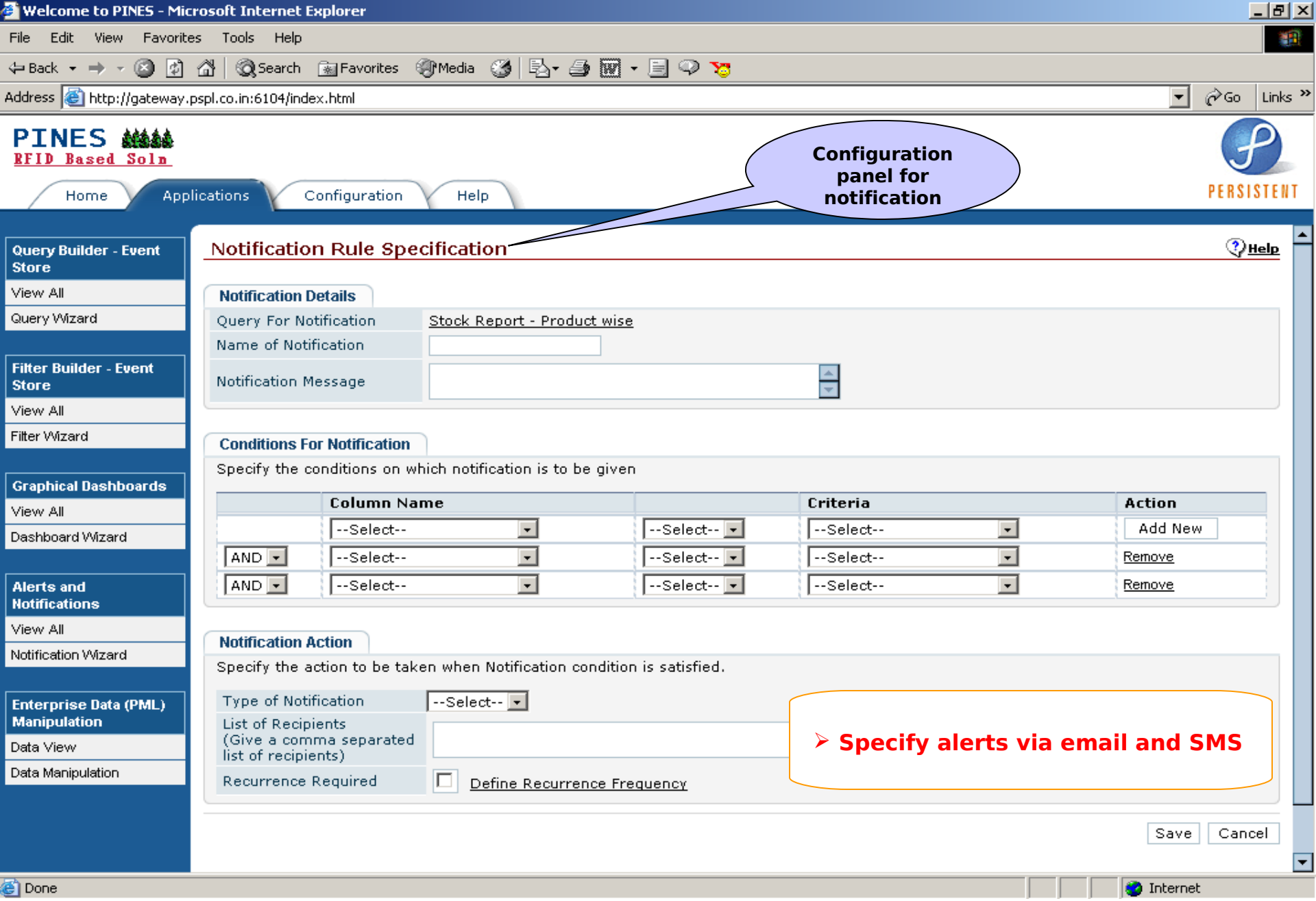


Source: **Persistent Systems**

Notifications

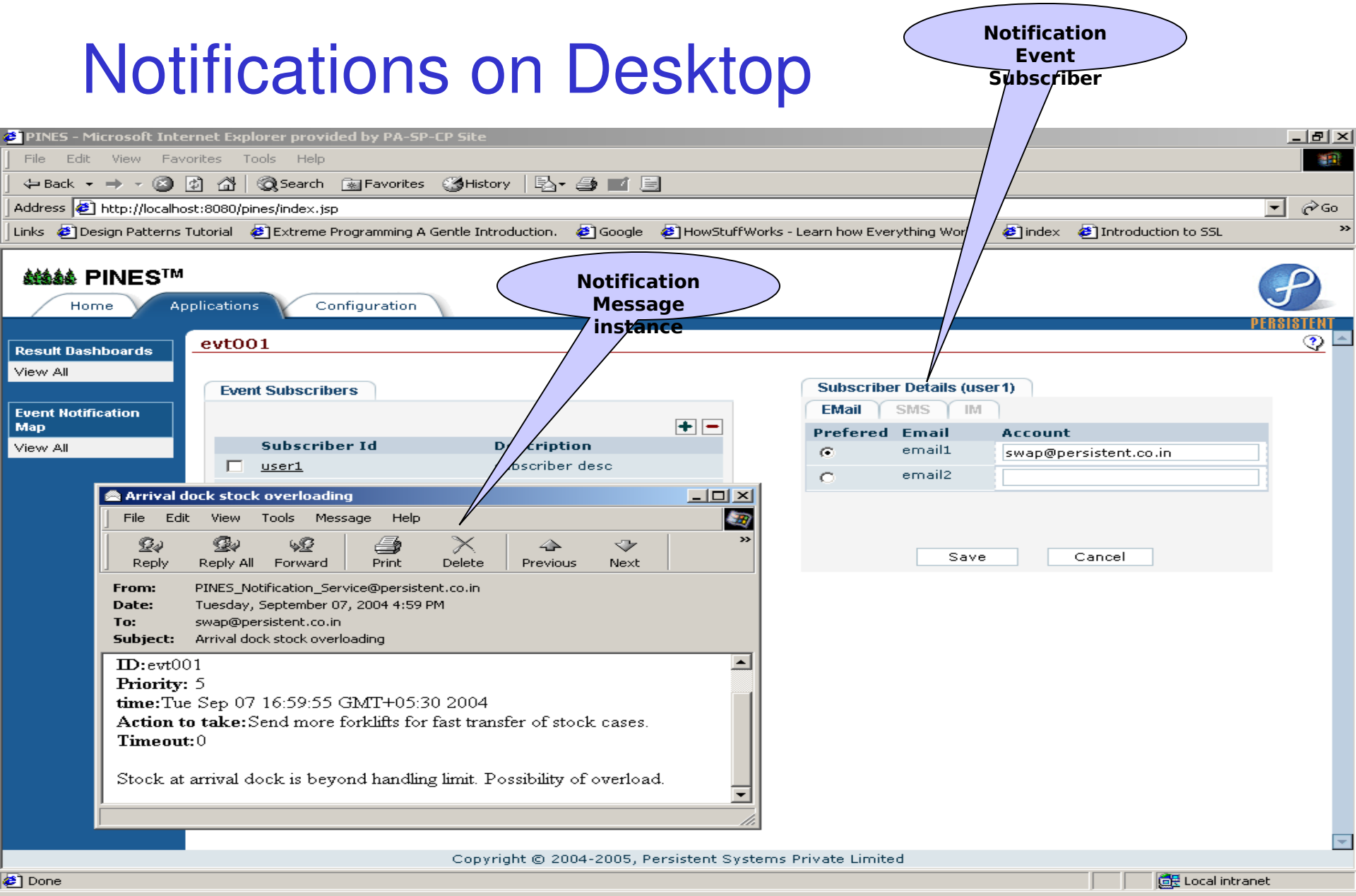
Notifications for enhanced decision making

Source: **Persistent Systems**



Source: **Persistent Systems**

Notifications on Desktop

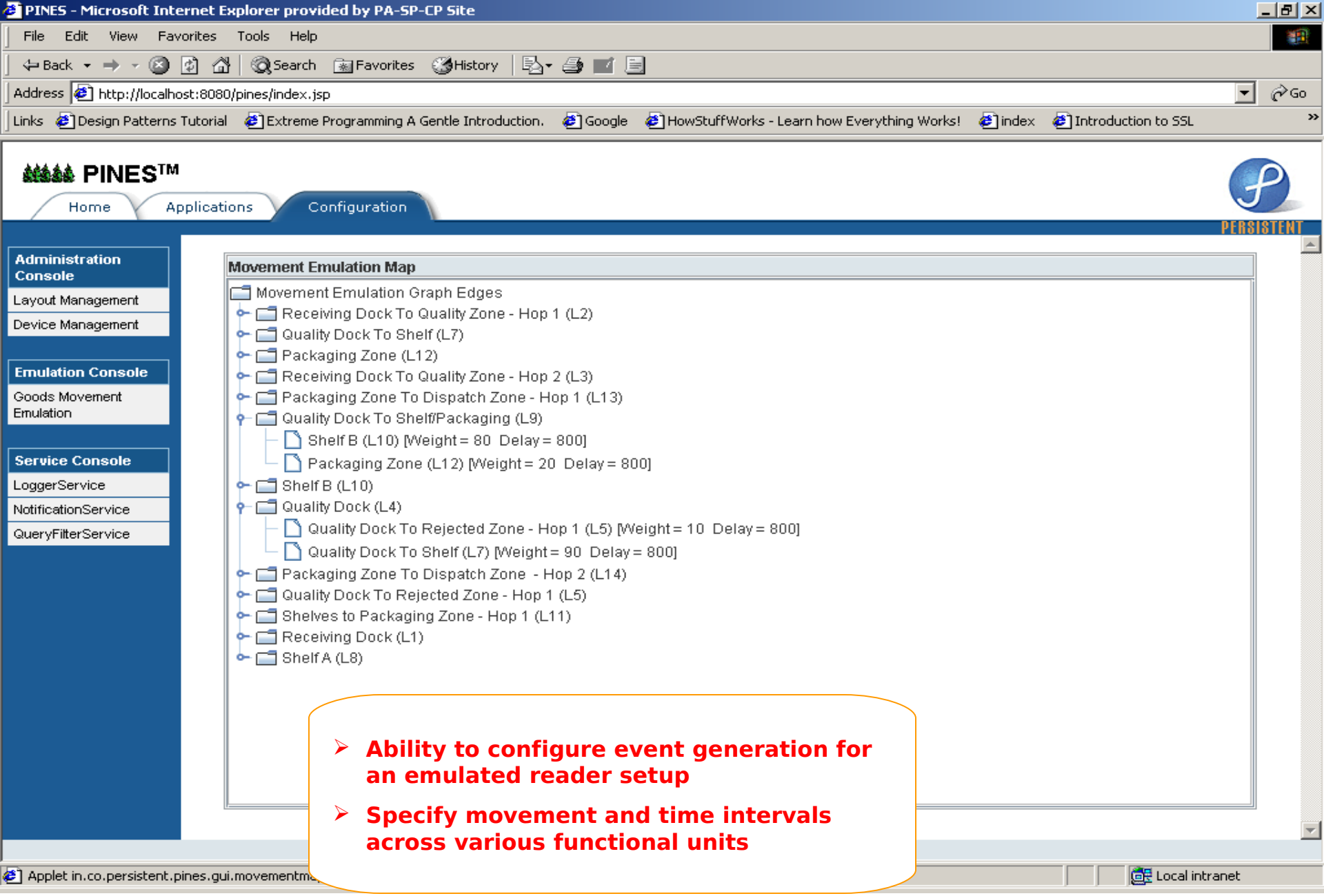


Source: **Persistent Systems**

Virtual Test Bed

Scenario emulation prior to deployment

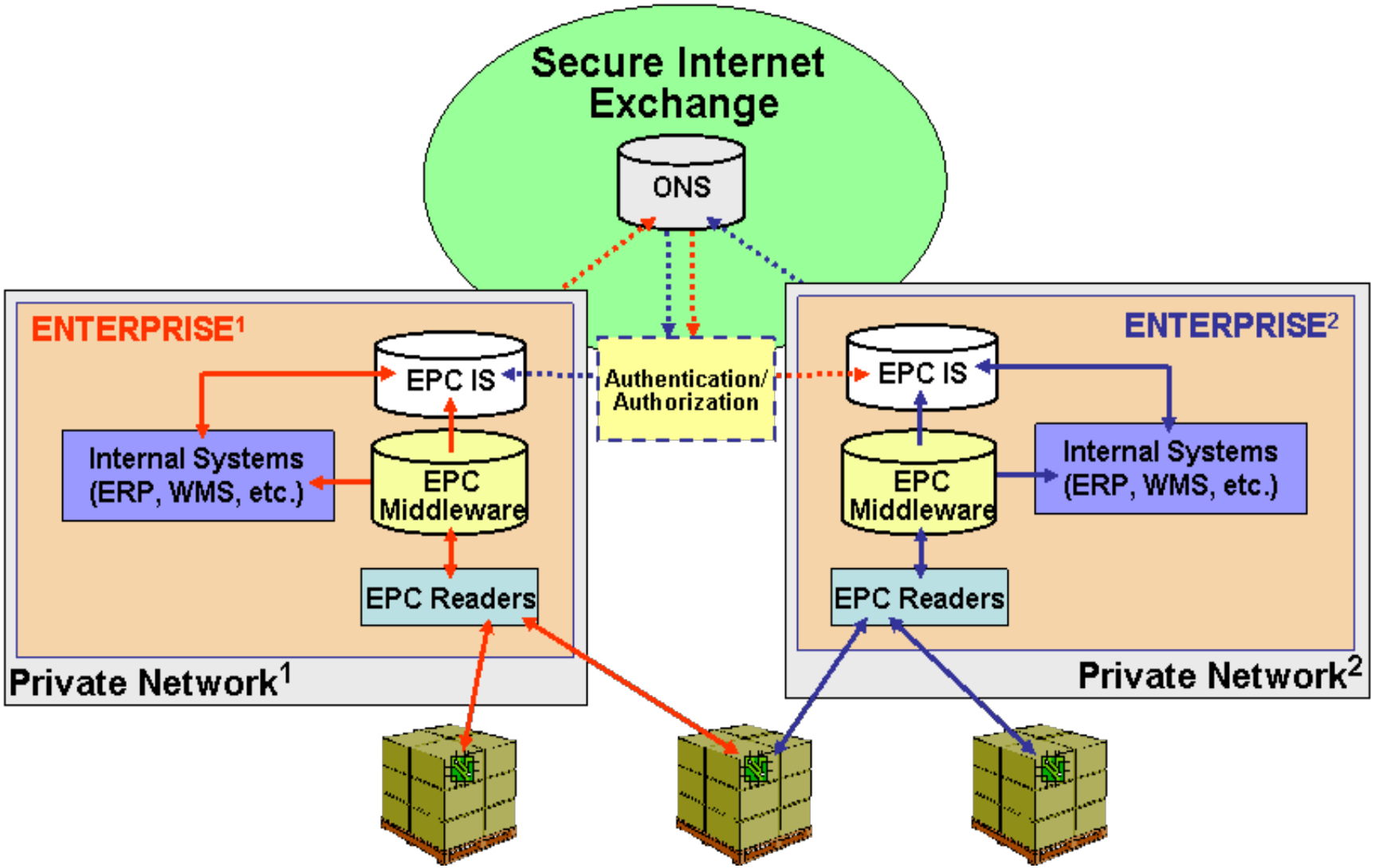
Source: **Persistent Systems**



- **Ability to configure event generation for an emulated reader setup**
- **Specify movement and time intervals across various functional units**

Source: **Persistent Systems**

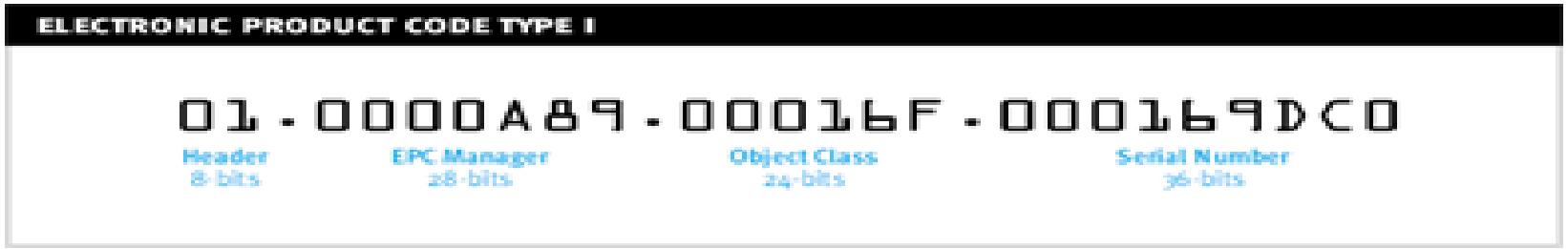
The EPC model: Internet of Things



Source: **www.epcglobalinc.org**

EPC and PML

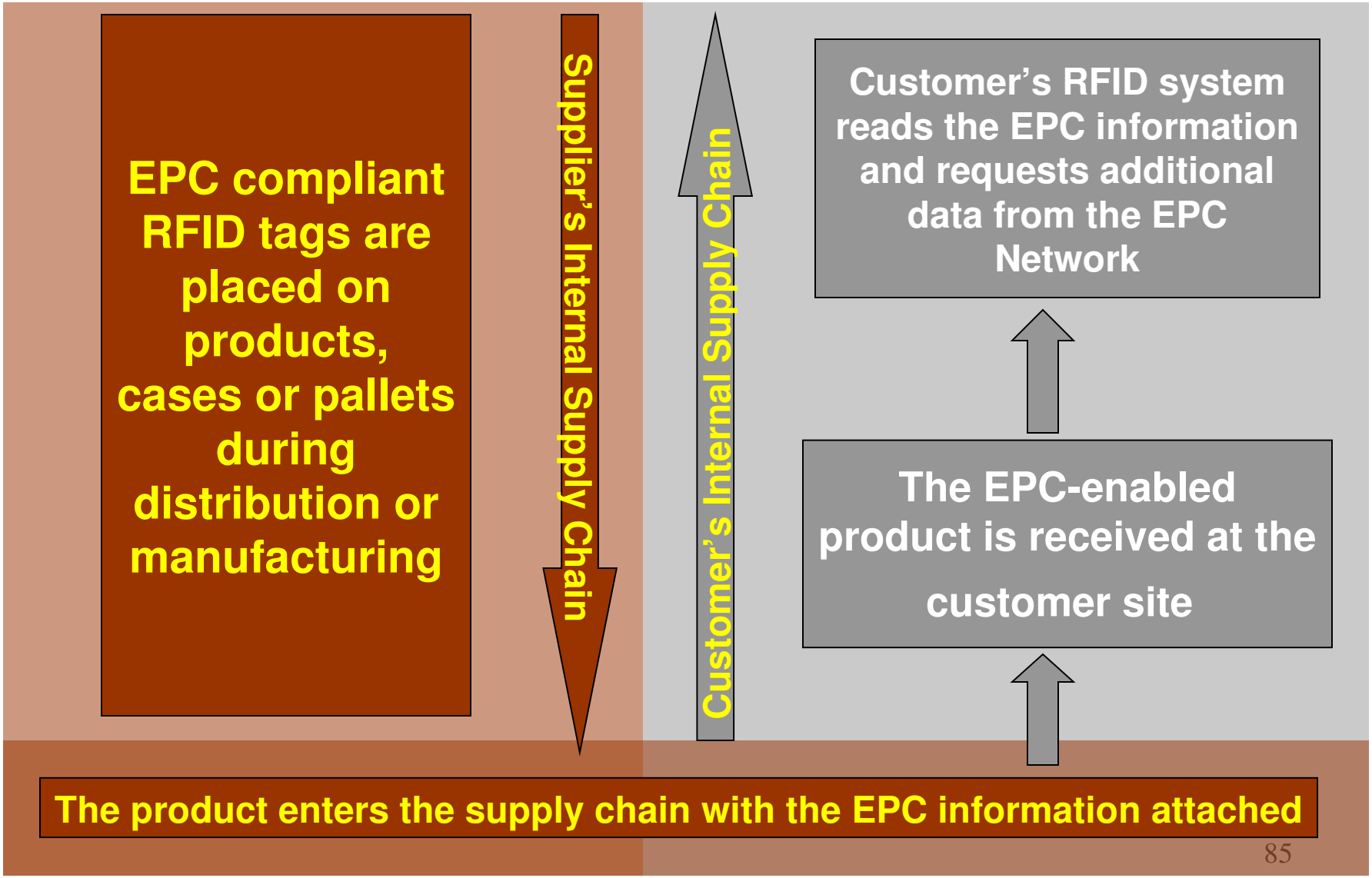
- EPC – Electronic Product Code
  - Header – handles version and upgrades
  - EPC Manager – Product Manufacturer Code
  - Object Class – Class/Type of Product
  - Serial Number – Unique Object Identity
- PML – Physical Markup Language
  - Extension of XML
  - Representation of Tagged Object Information
  - Interaction of Tagged Object Information



Savant and ONS

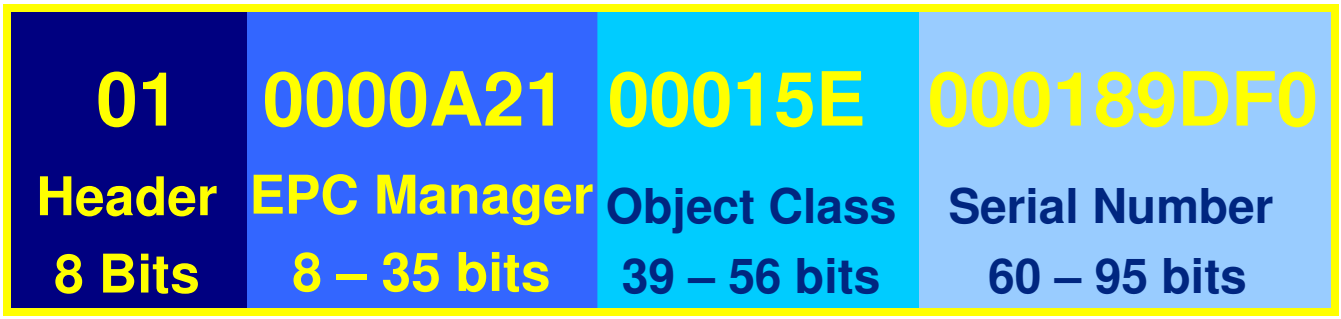
- Savants
  - Manage the flow of EPC data from RFID readers
    - Data smoothing
    - Reader coordination
    - Data forwarding
    - Data storage
  - Interact with the ONS network
- ONS Servers
  - Directory for EPC information, similar to Internet DNS
  - Uses the object manager number of the EPC to find out how to get more information about the product

EPC process flow



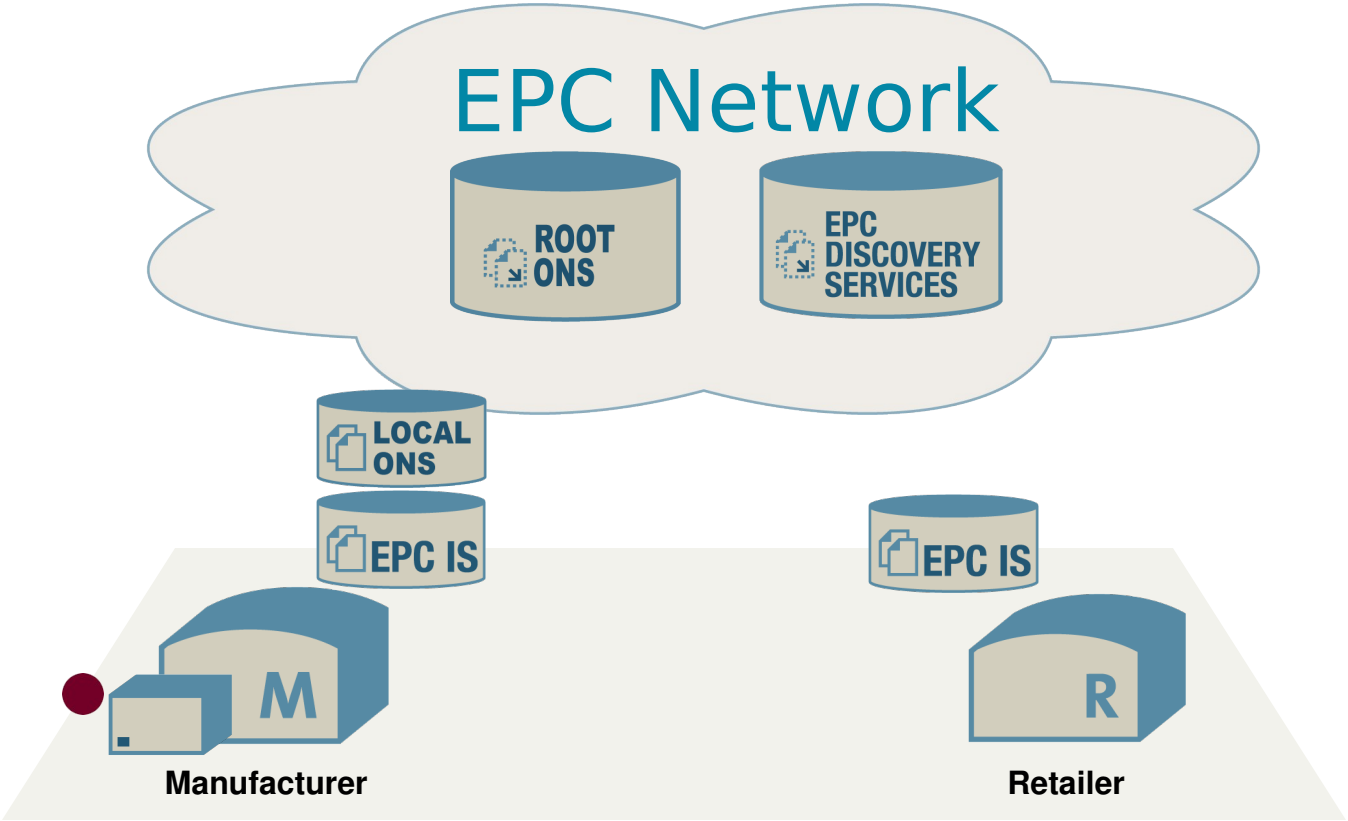
EPC Tags

64 and 96 bit EPC tags have been defined



- Allows for unique IDs for 268 million companies
- Each company can then have 16 million object classes
- Each object or SKU can have 68 billion serial numbers assigned to it

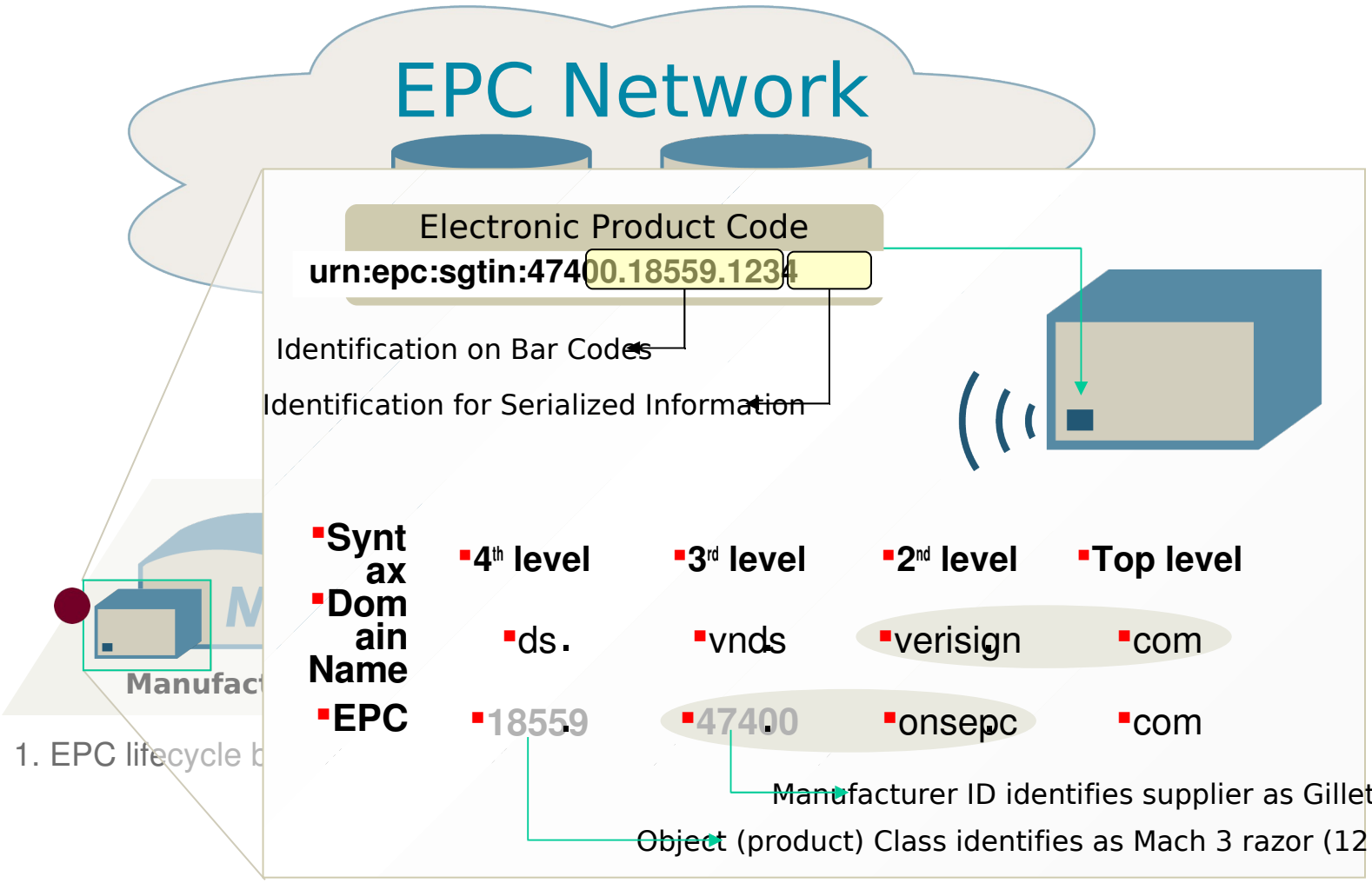
The EPC Network



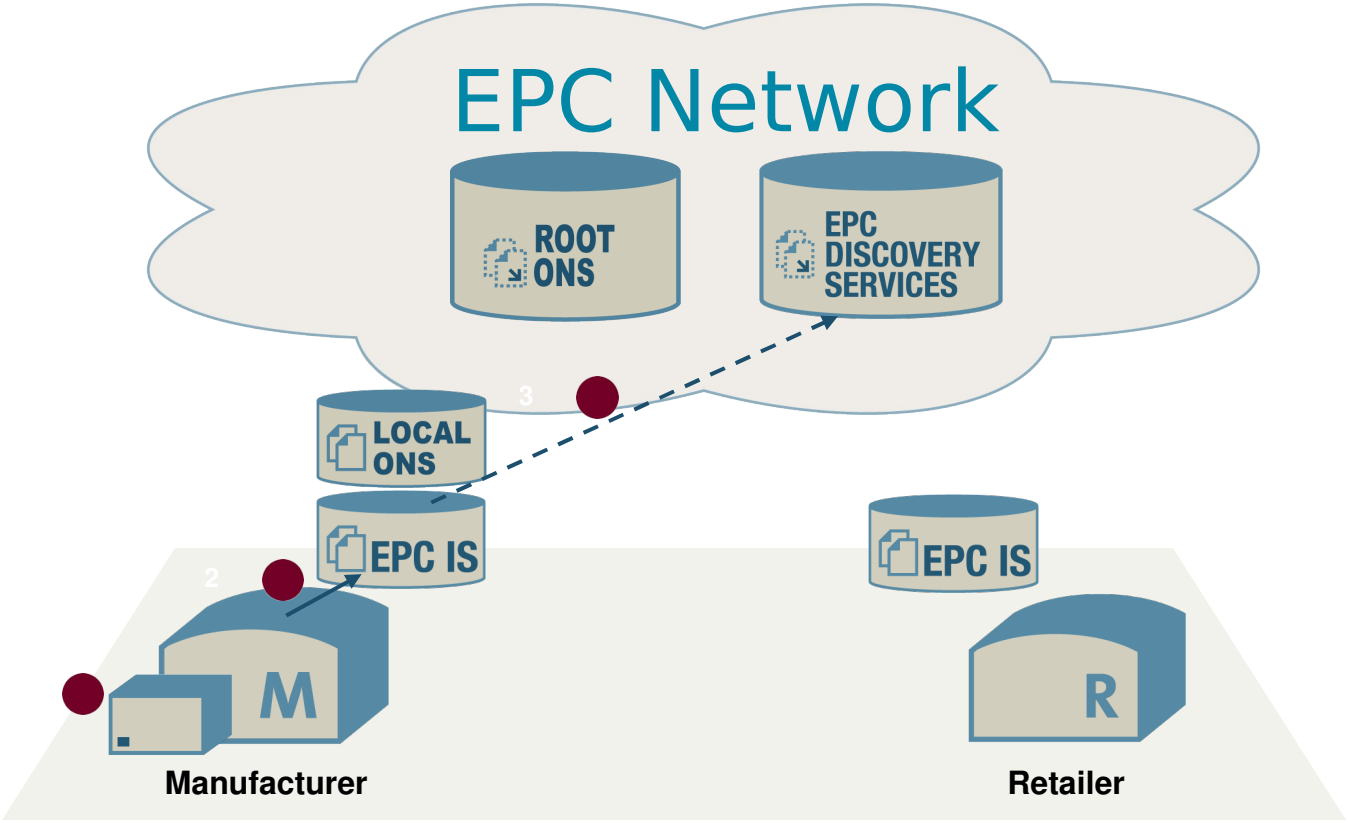
1. EPC lifecycle begins when a Manufacturer tags the product

Source: **Verisign Inc**

The EPC Network

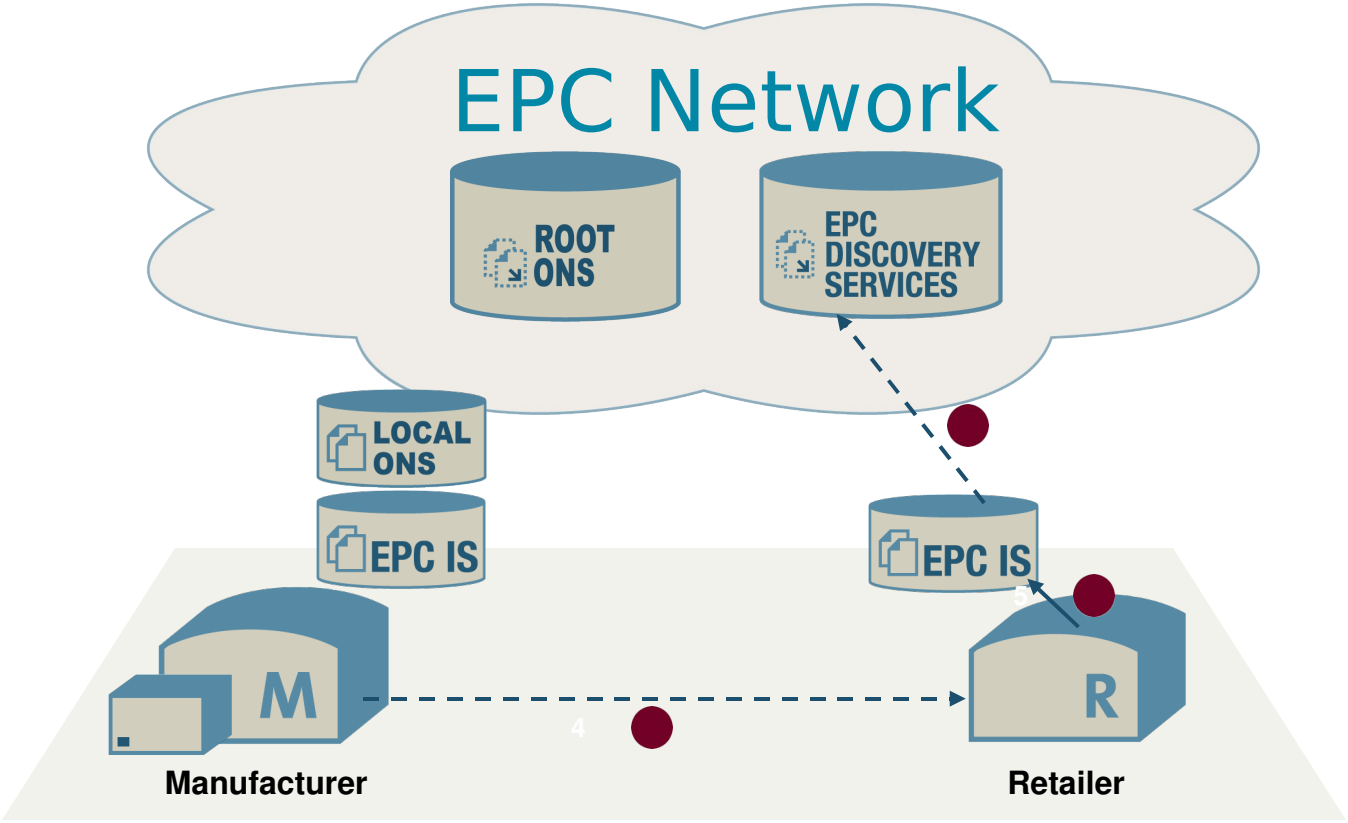


The EPC Network



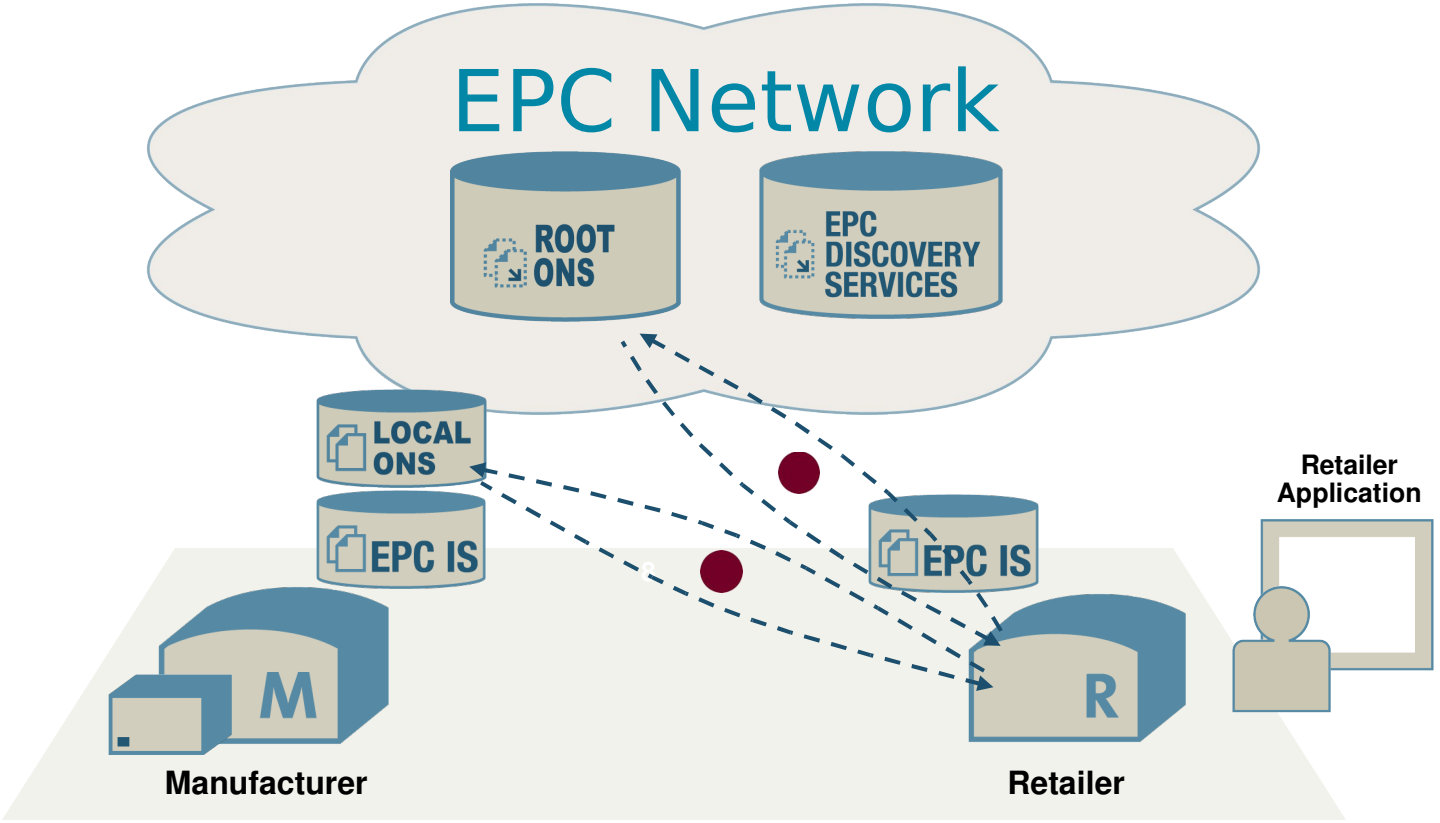
1. EPC lifecycle begins when a Manufacturer tags the product
2. Manufacturer records product information (e.g., manufacture date, expiration date, location) into EPC Information Service
3. EPC Information Service registers EPC “knowledge” with EPC Discovery Service

The EPC Network



4. Manufacturer sends product to Retailer
5. Retailer records “receipt” of product into EPC-IS
6. Retailer’s EPC-IS then registers product “knowledge” with EPC Discovery Service

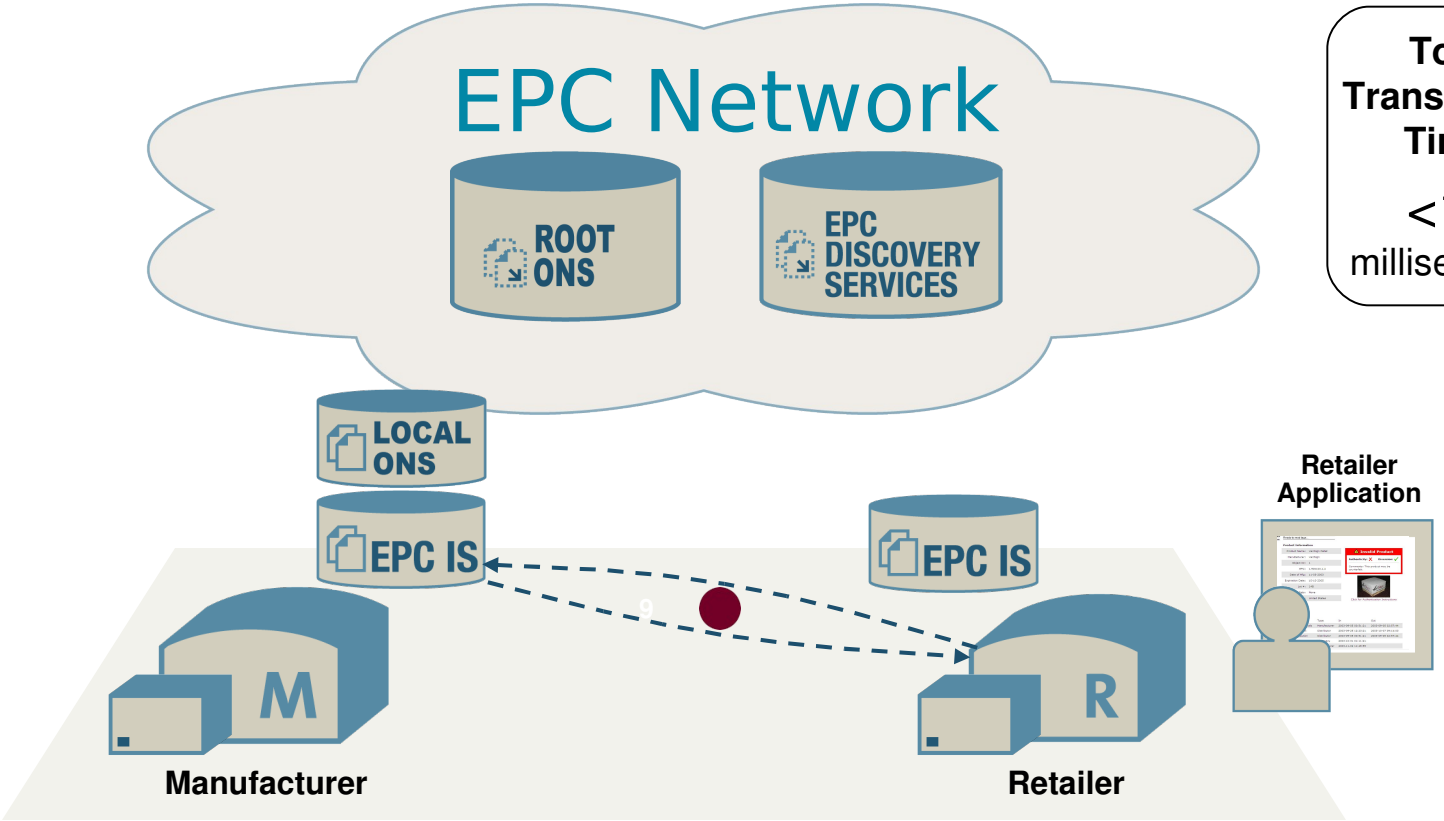
The EPC Network



7. If Retailer requires product information, Root ONS is queried for location of Manufacturer's Local ONS

8. Manufacturer's Local ONS is queried for location of EPC-IS

The EPC Network



Total Transaction Time:

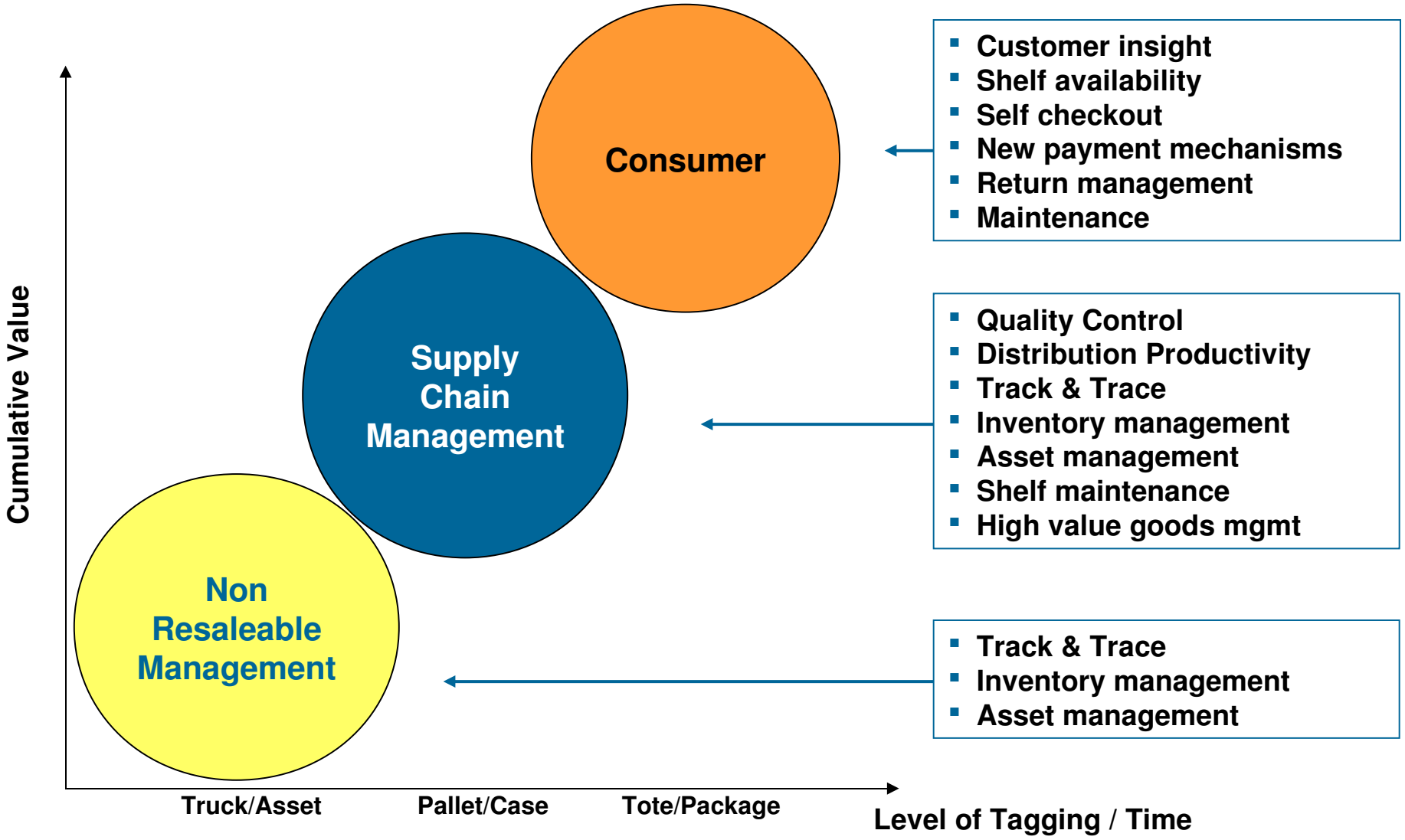
<10 milliseconds

9. Retailer queries Manufacturer EPC-IS for desired product information (e.g., manufacture date, expiration date, etc.)

Outline

- Overview of RFID
  - Reader-Tag; Potential applications
- RFID Technology Internals
  - RF communications; Reader/Tag protocols
  - Middleware architecture; EPC standards
- RFID Business Aspects
- Security and Privacy
- Conclusion

Business implications of RFID tagging



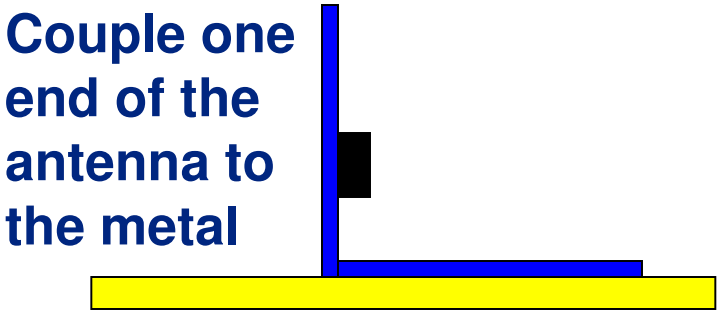
Source: **www.accenture.org**

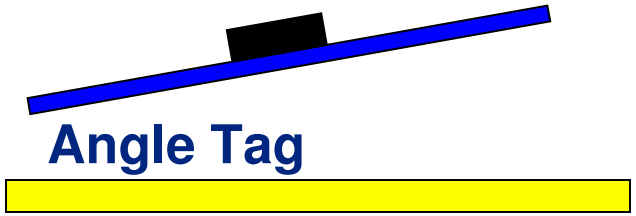
RFID deployment challenges

- Manage System costs
  - Choose the right hardware
  - Choose the right integration path
  - Choose the right data infrastructure
- Handle Material matters
  - RF Tagging of produced objects
  - Designing layouts for RF Interrogators
- Tag Identification Scheme Incompatibilities
  - Which standard to follow?
- Operating Frequency Variances
  - Low Frequency or High Frequency or Ultra High Frequency
- Business Process Redesign
  - New processes will be introduced
  - Existing processes will be re-defined
  - Training of HR
- Cost-ROI sharing

Using tags with metal

- Tags placed directly against metal will negatively affect readability

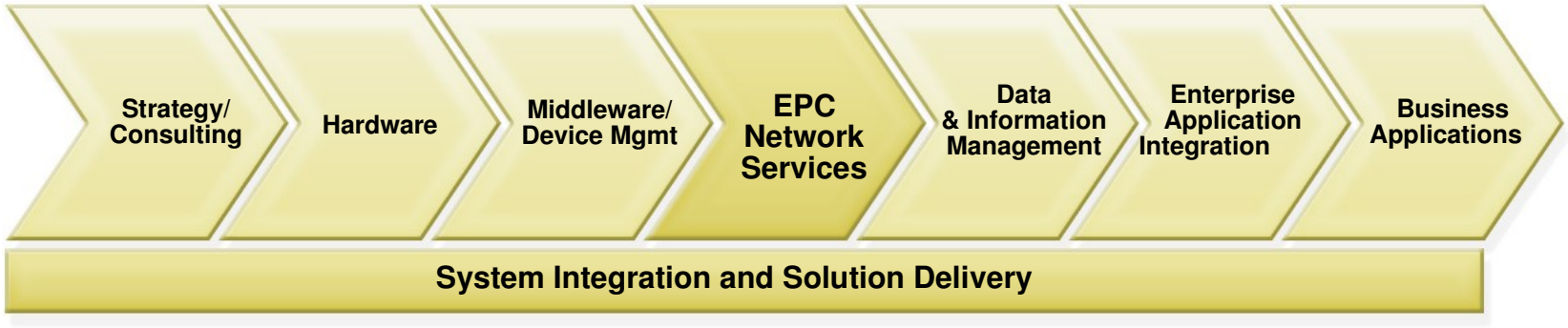




Getting ready for RFID

- Identify business process impacts
  - Inventory control (across the supply chain)
  - Manufacturing assembly
- Determine optimal RFID configuration
  - Where am I going to tag my components/products?
    - Surfaces, metal environment and handling issues
  - Where am I going to place the readers?
    - Moving from the lab environment to the manufacturing or distribution center can be tricky
  - When am I going to assemble the RFID data?
- Integrate with ERP and other systems

RFID services value chain



- Business Process Integration
- Solution Framework
- Network Setup
- RF aspects

- Tags
- Readers
- Label Printers

- Event Monitoring
- Data filtering
- Reader coordination
- Policy Management

- Directory Services
- Discovery Services
- Authorization / Authenticatn Framework

- Product Catalog and Attribute Managemnt
- Data Synchro-nization

- ETL Services
- Legacy Application Integration

- Supply Chain Execution
- ERP
- Warehouse Management
- Store Management
- Distribution Management

Source: **AMR Research**

Privacy: The flip side of RFID

- Hidden placement of tags
- Unique identifiers for all objects worldwide
- Massive data aggregation
- Unauthorized development of detailed profiles
- Unauthorized third party access to profile data
- Hidden readers

Source: **www.rfidprivacy.org**

The "Blocker" Tag approach

- "Tree-walking" protocol for identifying tags recursively asks question:
  - "What is your next bit?"

- Blocker tag always says ***both '0' and '1'***!
  - Makes it seem like *all* possible tags are present
  - Reader cannot figure out which tags are actually present
  - Number of possible tags is *huge*, so reader stalls

More on blocker tags

- Blocker tag can be ***selective:***
  - *Privacy zones:* Only block certain ranges of RFID-tag serial numbers
  - *Zone mobility*: Allow shops to move items into privacy zone upon purchase
- Example:
  - Blocker blocks all identifiers with leading ‘1’ bit
  - Items in supermarket carry leading ‘0’ bit
  - On checkout, leading bit is flipped from ‘0’ to ‘1’
    - PIN required, as for “kill” operation

The Challenge-Response approach

- Tag does not give all its information to reader.
  - The closer the reader, the more the processing.
  - Tag reveals highest level of *authenticated* information.

1. Reader specifies which level it wants.
2. Tag specifies level of security, *and/or* amount of energy needed.
3. Reader proceeds at that level of security.
4. Tag responds if and only if it gets energy and security required.

Some more approaches

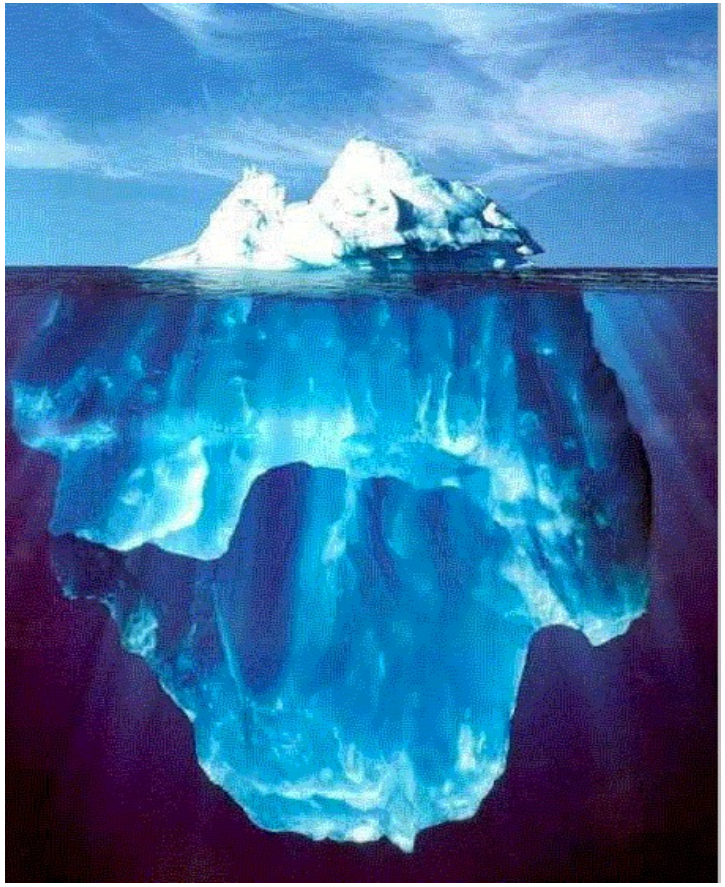
- The Faraday Cage approach.
  - Place RFID tags in a protective mesh.
  - Would make locomotion difficult.
- The Kill Tag approach.
  - Kill the tag while leaving the store.
  - RFID tags are too useful for reverse logistics.
- The Tag Encryption approach.
  - Tag cycles through several pseudonyms.
  - Getting a good model is difficult.

- No ‘one-size-fits-all’ solution.
- Security hinges on the fact that in the real world, an adversary must have physical proximity to tags to interact with them.

Outline

- Overview of RFID
  - Reader-Tag; Potential applications
- RFID Technology Internals
  - RF communications; Reader/Tag protocols
  - Middleware architecture; EPC standards
- RFID Business Aspects
- Security and Privacy
- Conclusion

RFID: The complete picture



Tags and Readers

Identifying Read Points
Installation & RF Tuning
RFID Middleware
Connectors & Integration
Process Changes
Cross Supply-Chain View

Points to note about RFID

- RFID benefits are due to automation and optimization.
- RFID is not a plug & play technology.
- “One frequency fits all” is a myth.
- Technology is evolving but physics has limitations.
- RFID does not solve data inconsistency within and across enterprises.
- Management of RFID infrastructure and data has been underestimated.

RFID Summary

Strengths	Weaknesses
➢ Advanced technology ➢ Easy to use ➢ High memory capacity ➢ Small size	➢ Lack of industry and application standards ➢ High cost per unit and high RFID system integration costs ➢ Weak market understanding of the benefits of RFID technology
Opportunities	**Threats**
➢ Could replace the bar code ➢ End-user demand for RFID systems is increasing ➢ Huge market potential in many businesses	➢ Ethical threats concerning privacy life ➢ Highly fragmented competitive environment

Some Links

- http://www.epcglobalinc.com/
- http://www.rfidjournal.com/
- http://rfidprivacy.com/
- http://www.rfidinc.com/
- http://www.buyrfid.com/

Thank You