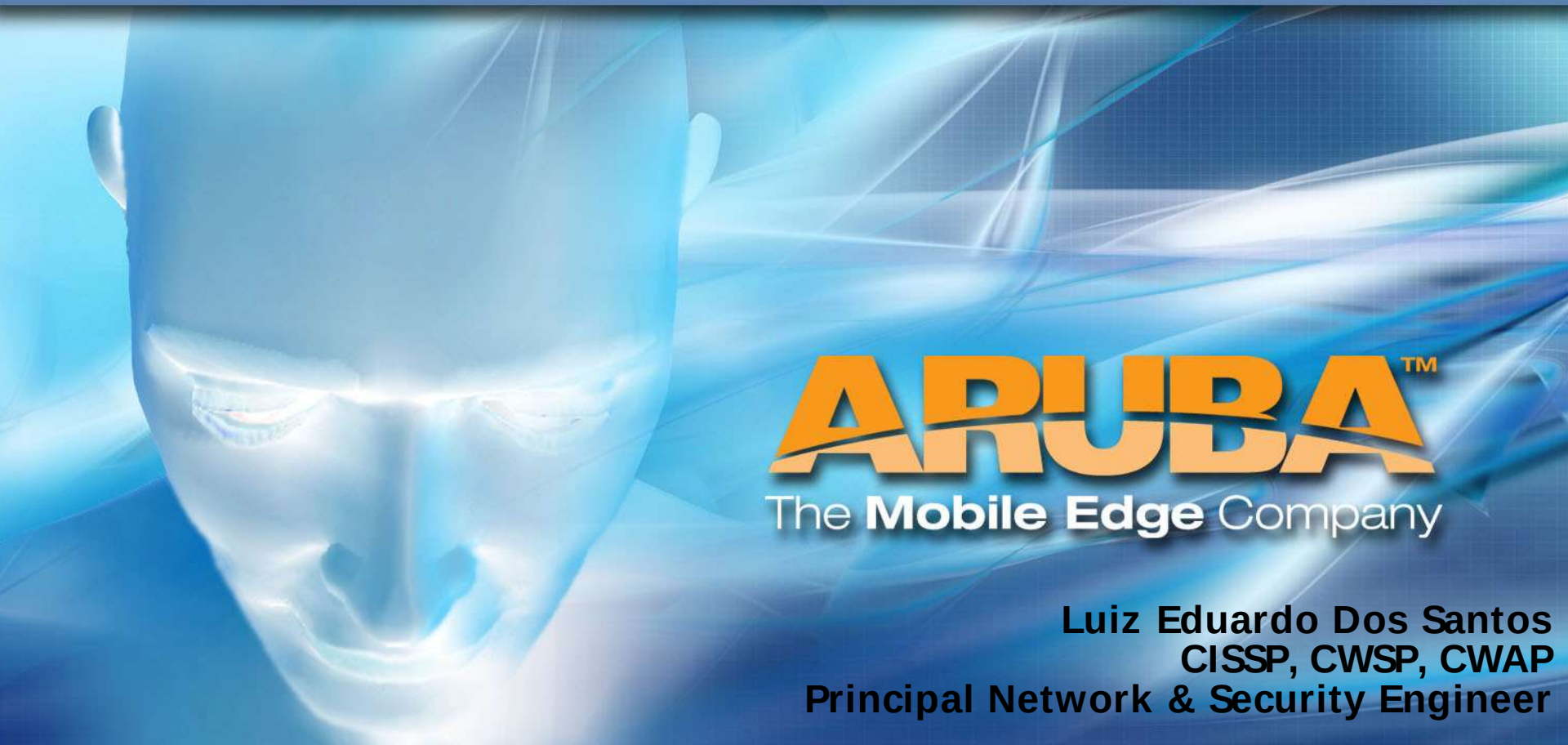
RF- ID Tecnologia, Segurança e Privacidade
GTS Reunião 02.05



Luiz Eduardo Dos Santos
CISSP, CWSP, CWAP
Principal Network & Security Engineer

What is RF- ID and why?

- Radio Frequency Identification
- “Derived” from the RADAR technology
- Inventory control (barcode replacement?)
- Active and passive tags
- Detect misplaced products and expired goods

Facts

- There are different types of tags
- Some have some sort of write protection
- Up to 1000 write cycles
- Each tag carries an unique identifier
- Some stores require suppliers to have products with RFID

Myths

- RFID will replace barcode
- RFID is just a “talking” barcode (nope, up to 2kB of info)
- Tags can be read from a long distance

RFID technologies & applications

While both are called 'RFID', Wi-Fi tag location and UHF tag location are different technologies

- Used to locate mobile items
- Two different technologies
  - Wi-Fi Tags
  - UHF 'RFID' passive tags
- Differing range, cost, capabilities

UHF RFID tags work at 915 MHz.
They are inexpensive,
usually passive (no batteries)
but very short-range

UHF RFID tag applications

- Wholesale/retail distribution chain
- Carton-level tagging through the supply chain (groceries)
- Item-level tagging of high-value items (razor blade packages)
- Real-time checking of truck loading
- Homeland security implications of an audit chain for foodstuffs
- Manufacturing
- Potential to replace bar-codes

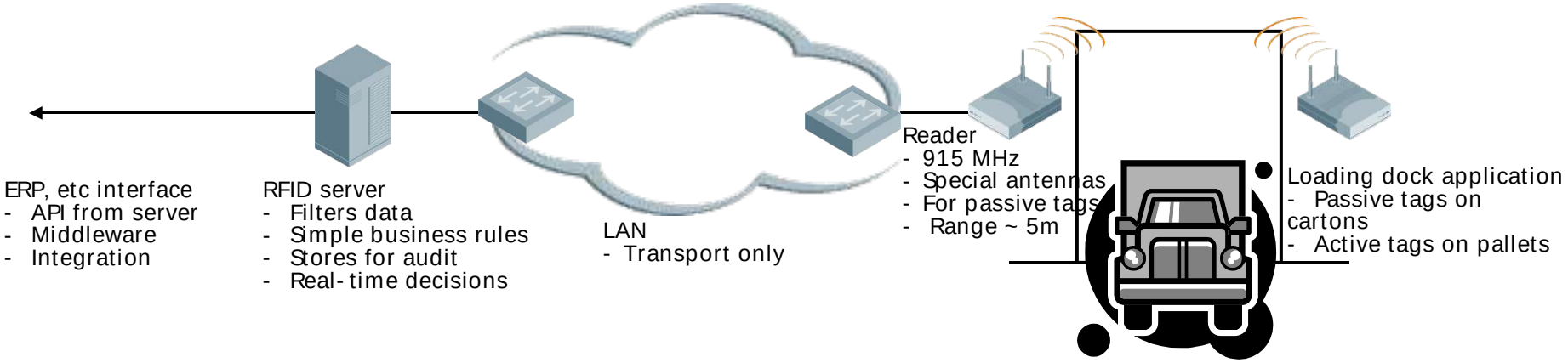
Wi-Fi tags work at 2400 MHz.
They are expensive,
active (batteries with relatively short life)
and longer-range

Wi-Fi tag applications

- High-value mobile equipment
- IV pumps & other equipment in hospitals
- Patients in hospitals
- Manufacturing (aero engines)
- Shipping industry (rail cars, shipping containers)
- Identify IT equipment in server farms
- Locate mobile equipment for on-site maintenance

RFID technologies – UHF

UHF tags are sub-$, but have very short range… used at traffic choke points to detect flow



Technology

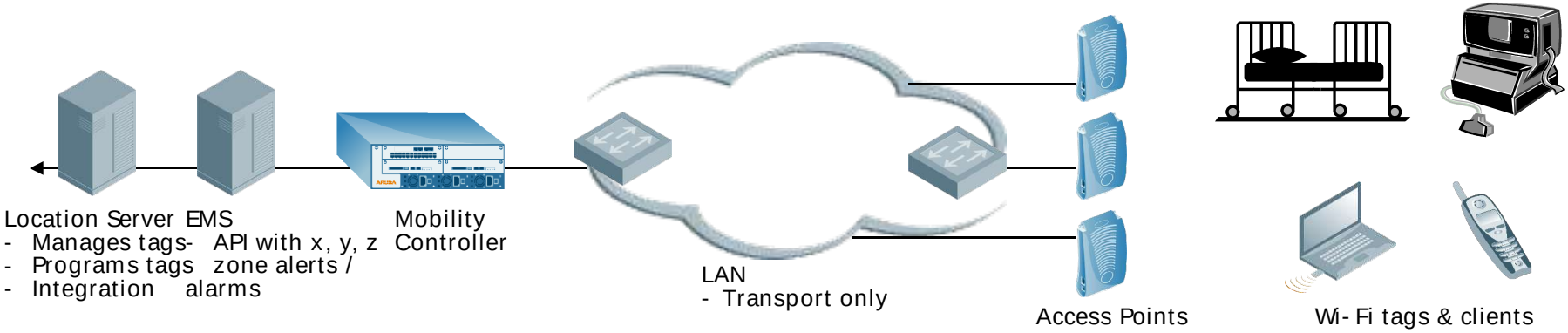
- Passive tags
  - Low-cost
  - Low-complexity
  - Carry UPC-like information
- Radio requirements
  - 902-928 (915) MHz
  - RF transmissions excite tags
  - Tags return information to reader
- Traffic characteristics
  - Many transactions, little data per transaction
- Back-end integration requirements
  - ERP & business systems integration

Characteristics & Issues

- Cost of tags (~50c but still too high)
- Cost of readers (~$1000 installed)
- Short range of detection (~2 meters)
- Not re-programmable
- Duplicate reads
- Missed reads & RF coverage holes
- Detecting vector motion (direction through a doorway)
- Management, coordination of many readers
- Middleware & ERP integration
- Immature technology – emerging reader architectures
- Business case difficult

RFID technologies – Wi- Fi Tags

Wi- Fi tags are more expensive (~$50), but can be detected over much longer ranges



Technology

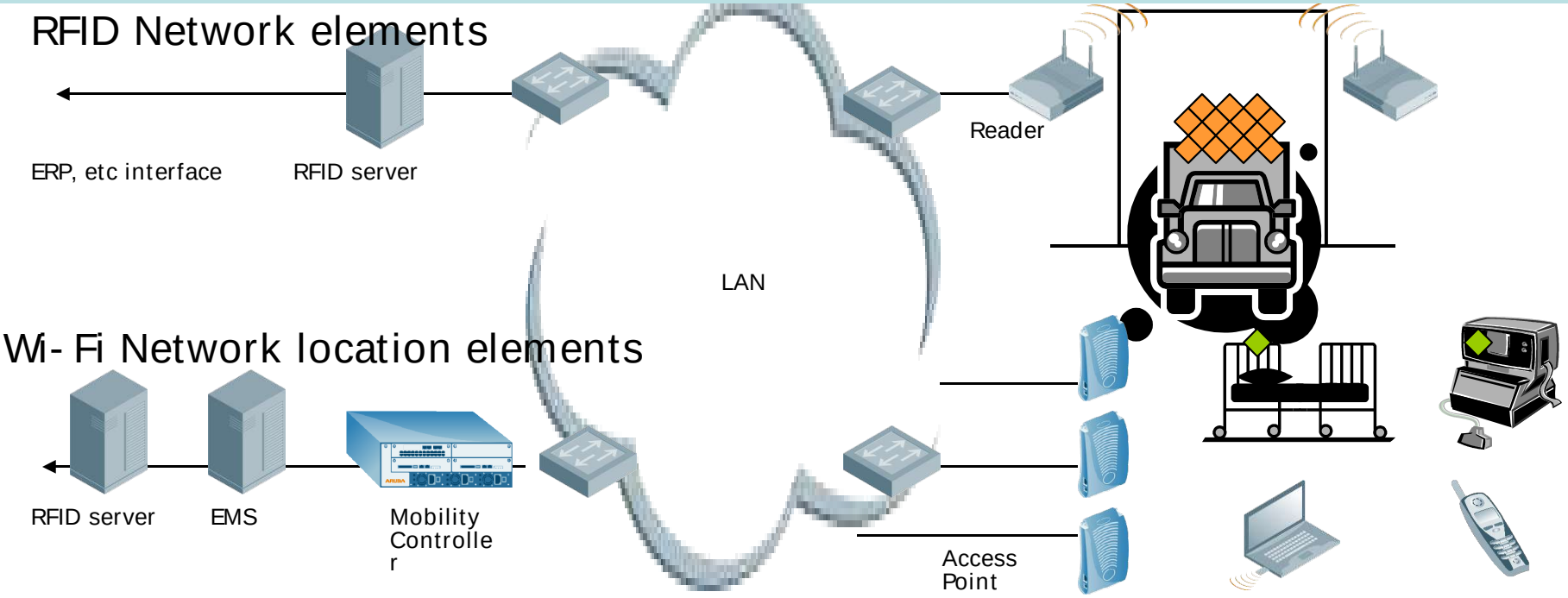
- Wi- Fi tags
  - High- cost
  - High- complexity (need programming)
  - No standard for data format
- Radio requirements
  - Wi- Fi
  - Association or 'Blink'
  - Longer range than UHF: 20+ metres
- Traffic characteristics
  - Few transactions, larger data sets
- Back- end integration requirements
  - Usually standalone business- rules engine
  - Any Wi- Fi client can be tracked, located

Characteristics & Issues

- Cost of tags (~$50)
- Range (~ 30 meters)
- Lack of standards
- Battery life (~1 year)
- Number of servers, complexity of administration
- Lack of inter- vendor interfaces
- Middleware, business rules integration
- WLAN architecture is mature
- Business case difficult

RFID Integration Myths

Integration between UHF RFID and Wi-Fi location infrastructures is at a very early stage

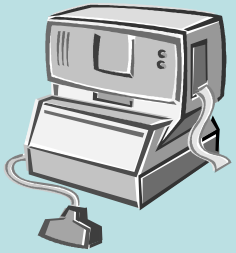


- No vendor has yet integrated the two RFID technologies
- Much slideware, no concrete development
- No vendor builds and sells integrated Wi-Fi AND UHF RFID infrastructure
- No vendor sells a server that tracks both Wi-Fi AND UHF RFID tags
- Extent of current integration is running both systems over a common LAN

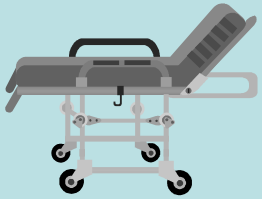
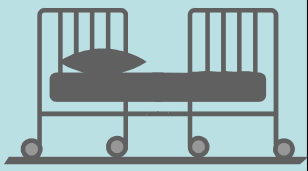
RFID & Location Technologies in Healthcare

Hospitals have many requirements for tags for Wi-Fi location and telemetry, as well as locating other Wi-Fi equipment (phones, bar-code scanners, tablet PCs, patient monitoring stations)


Wi-Fi tags on doctors and nurses, for audit (when was the patient last visited?) and on patients to make sure they do not stray (e.g. Alzheimer's, infectious diseases)

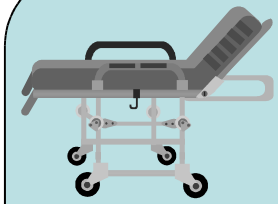
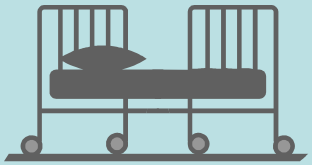
Wi-Fi tags on to mobile equipment (also reporting status, e.g. fluid levels in order for maintenance engineers to identify and locate

Wi-Fi tags on mobile assets in order for
nurses to locate them (also reporting start/end of motion)

And for UHF RFID


UHF RFID tags can identify medicines, for matching to patient at point-of-delivery

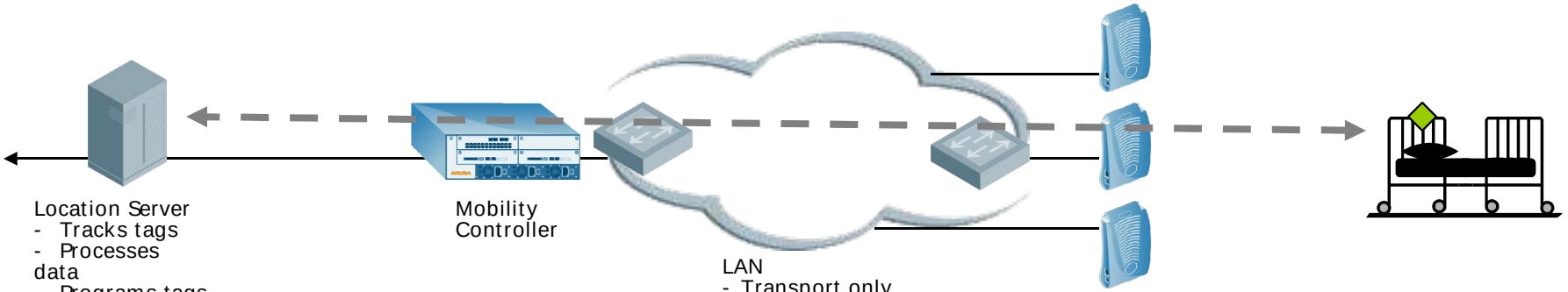



UHF RFID tags are useful for flow monitoring (e.g. alarms on passing through a doorway)


Active tags (UHF or Wi-Fi) can detect and report when material has been stored over-temperature or suffered other mis-handling

First- generation Wi- Fi tags

Many tags on the market today are first- generation, second- generation is just emerging



5 – Location Server integrates with IT applications (inventory, maintenance, nurse call, etc) as middleware

3 – Location server processes RSSI information, compares to site fingerprint and determines location

2 – tag associates, authenticates and connects to the location server

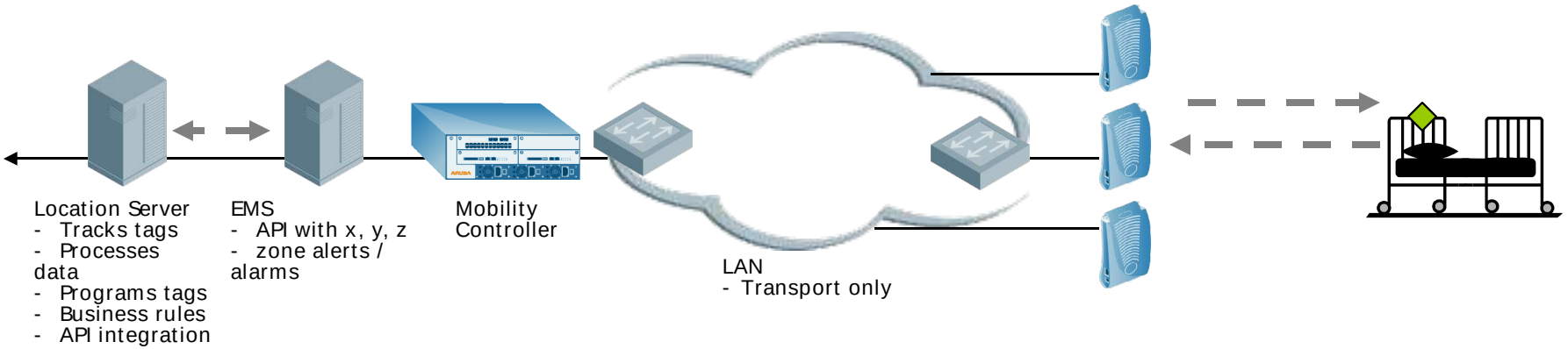
1 – tag wakes up (on clock or motion) and listens for AP's on all Wi- Fi channels, logs RSSI

- Operates as an overlay over the WLAN infrastructure
- Requires long transmit times
  - 802.11 association for every transmission
  - Rather poor battery life
  - Large tag profile

4 – tag may be reprogrammed, firmware- updated, or report more detailed telemetry information, battery state, etc

Second- generation Wi- Fi tags

Second- generation improvements: Over- the- air interface, location server API



4 – Location Server no longer derives location , only applies business rules & tag programming

3 – network determines tag location, reports x, y, z

2 – network detects blink at multiple APs

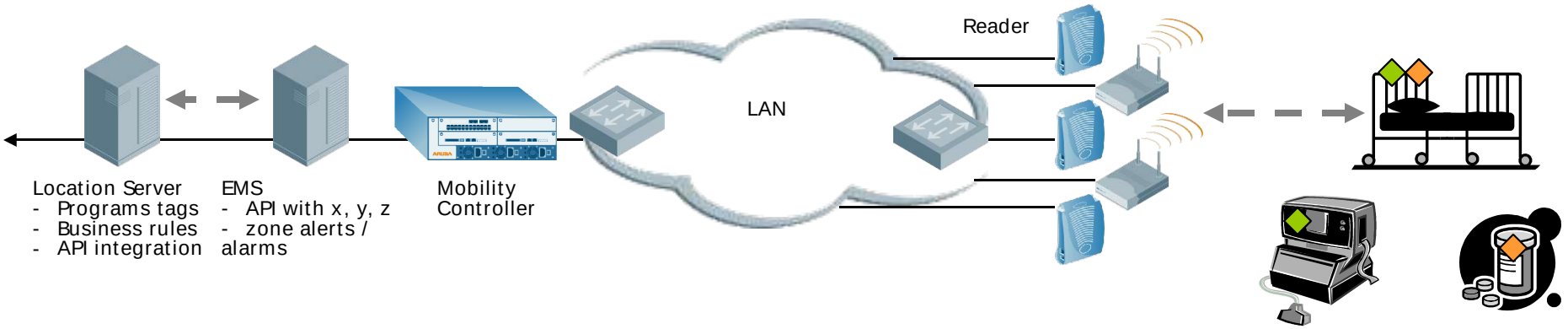
1 – tag blinks with pre- determined frame

5 – New downlink frames allow simple reprogramming of the tag without association (e.g. channels, blink rate)

- Greatly improved battery life
  - No association required
  - Smaller tag profile
- Simplified Location Server
  - WLAN infrastructure provides xyz on API
- Standardization opportunity
  - Mix- and- match tags & Location Servers & WLANs

Future Generations of RFID

Several opportunities for integrating infrastructure and technology



5 – Location server correlates between signals from UHF, Wi-Fi APs

4 – Mobility controller manages UHF readers as well as Wi-Fi APs

3 – WLAN determines tag location, reports x, y, z

2 – integrate Wi-Fi, UHF readers / APs for simplicity & cost savings

1a – Wi-fi only tags

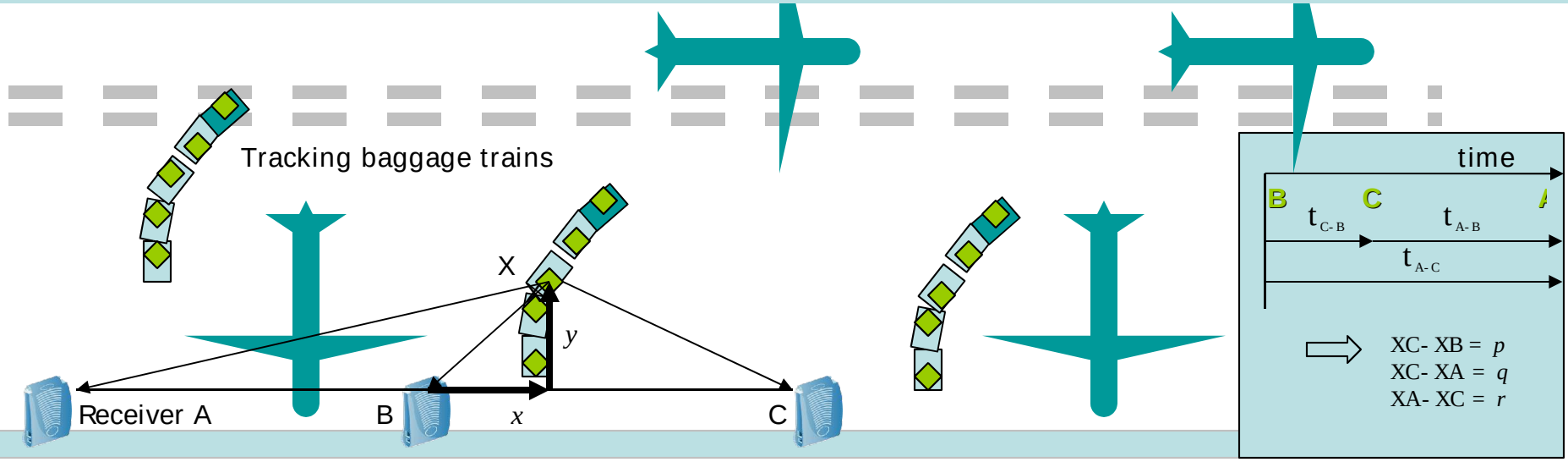
1b – UHF RFID tags

1c – combined technology tag (Wi-Fi, Bluetooth, UHF) allows wide-area detection & accuracy where it counts

- Multi-technology network
  - Single mobility controller architecture for UHF readers, Wi-Fi APs
- Multi-technology tags
  - Wi-Fi for range, UHF/Bluetooth for proximity
  - Expense constraints
- Unified Location Server
  - Single server handles UHF & Wi-Fi & combination tags

TDOA Location Technologies

Use standard Wi-Fi tags, but require special receivers: good outdoors



- TDOA (Time Difference of Arrival) accuracy is constant (dependent on the accuracy of time measurement, 1ft/nsec)
  - Accuracy of 10nsec is 10ft, regardless of distance measured: 10ft whether the measurement is 60ft or 180ft
- RSSI accuracy is proportional to distance
  - 25%of 60ft is 15ft, 25%of 180ft is 45ft
- Outdoor usually means long distances from tag to AP, so TDOA is often preferred
- TDOA technology requires special receiver hardware today
- Combined Wi-Fi AP with TDOA receivers are available, but expensive
- Mobile RF obstacles (e.g. planes, catering trucks) create shadows & multipath, so accuracy can vary
- Shadow, multipath effects may affect RSSI more than TDOA

Today's RF- ID Applications

- Inventory control (product tracking)
- People tracking (parks/ clubs)
- Car keys
- Access control (badges)
- Luggage tracking
- Passports / immigration documents
- Customer loyalty cards
- Toll collection
- Libraries
- Exxon's Speedpass
- Cattle tracking

“New” RF- ID Applications

- MP3 player with smartcard
- Clothing
- Vending machines
- Casino chips
- Cellphones

Future RF- ID Applications

- Home appliances (refrigerators, washers, “smart” ovens)
- Money
- Smart paper (books, business cards)
- And many more to come...

Security Concerns

- No encryption
- User data memory can be modified
- No read protection
- No “scanning” protection

Privacy Concerns

- Eavesdropping (customer AND business privacy issues)
- “better” customer profiling
- Possible person identification (since the tag has no read protection)
- “hotlisting” based on products you are carrying (books, etc)
- Collection and use of PII (personally indentifiable information)
- 21st century dumpster dive

Privacy – again… Imagine..

- Where you go
- What you buy
- What you don't buy
- Data mining
- Store sends you targeted ads
- But…

Possible Solutions

- Kill the tag once it leaves the store
- RSA's blocker tag
- Lock unused memory on the tag
- Use of encryption (?)

Attacks

- RF- Dump
  manipulates user data on the tag
- Tag swapping
- Convert products EPCs
- RF- ID Bombs

Resources

- http://www.rf-dump.org/
- http://www.spychips.com/
- http://www.nocards.org/
- http://www.rfidjournal.com/
- http://www.boycottgillette.com/

Obrigado

luiz AT arubanetworks.com