

Planning for Proliferation: The Impact of RFID on the Network

Analyst: Duncan Brown and Evelien Wiggers

An IDC White Paper

March 2005

Sponsored by: Cisco



WHITE PAPER

Planning for Proliferation: The Impact of RFID on the Network

Sponsored by: Cisco

Duncan Brown

Evelien Wiggers

March 2005

IDC OPINION

Radio frequency identification (RFID) is a network edge technology that impacts on the design and usage of network infrastructures. Though many RFID projects are in the early stages, it is in the nature of RFID to proliferate, both within an organisation's boundaries and throughout the supply chain. It is essential that organisations deploying RFID take a broad view of network impact and build scalability into their plans sooner rather than later.

Predicting the impact of RFID on pre-existing network infrastructure is complex. There are three main influencers that determine the size and direction of the impact:

- ☒ The degree of sophistication of the business objectives that drive the RFID solution
- ☒ The extent of integration of an RFID system with external parties in a supply chain
- ☒ The granularity of an entity tracked using RFID, with impact increasing as granularity increases (e.g., from container to pallet to case to item).

Impact includes not only increases in bandwidth but also variations in the network architecture itself: this includes device density and management; data storage; application-level event generation and routing; and network security.

IDC research reveals that most organisations begin their RFID adventure in a very localised environment, trialing the technology in small internal pilots. They may involve a close partner in order to test the possibilities for data exchange between organisations in the supply chain.

Our research also shows that organisations must start thinking **now** about the impact of RFID on the network when they implement, and integrate with, larger RFID systems. Scalability is a function of network *architecture*, not simply a matter of adding routers and switches, and it must be planned.

RFID deployments are extensive in scope and scale, requiring the tight integration of hardware and applications within an end-to-end network. Security is an integral element of RFID infrastructure, and it spans both wireless and wireline networks. This creates many challenges for the network. But there are also opportunities to benefit from the latest generation of network technologies. These can monitor real-time data at the network edge, provide the highest level of security and provide the sophistication required to implement RFID in a manageable way.

RFID will have a significant impact on organisations' internal processes, business models and technology infrastructures. RFID is an inevitability: organisations must assess the impact on their networks at this early stage, in order to take advantage of the substantial benefits as the technology matures.

Methodology

This IDC White Paper has been informed by a series of interviews with leading adopters of RFID technology, primarily in the retail, logistics and distribution sectors. Comments from these organisations have been added to by considering Cisco's activities in incorporating RFID capability within its network infrastructure product sets. IDC has also contributed its extensive research into networks and RFID adoption.

For this paper IDC specifically interviewed:

- ☒ CHEP: a global logistics firm. CHEP deploys containers and pallets across the globe, and requires sophisticated tracking of its assets.
- ☒ DHL: a global delivery company. DHL sends parcels, pallets of goods and other items to addresses around the world.
- ☒ House of Fraser: a premium brand department store chain in the UK. House of Fraser operates 50 stores in the UK, and sources its goods from around the world.
- ☒ A large high street retailer (wishing to remain anonymous). It sources its products from a variety of manufacturers and distributors, and sells them in its network of 600 stores in the UK and Ireland.
- ☒ Metro: the third largest retailing and wholesale group, operating in 30 countries and 2,500 locations.

IDC also drew on its substantial research on RFID deployments from the following companies: Ahold, Tesco, Metro, Kraft, Unilever, Marks & Spencer, Carrefour, Airbus, Boeing, Nestle, Delhaize, Gillette and REWE.

THE BENEFITS OF RFID

Hype surrounding RFID is as pervasive as RFID itself aims to be. Underpinning the hype, though, are promises of real operational improvements, particularly in the supply chain for the retail, logistics and manufacturing industries.

There are five primary reasons why organisations adopt RFID technology:

- ☒ Improved control of stock and other assets as they move within the organisation. This includes both movement of goods through a distribution network and the movement of goods through various stages of manufacture.

A large high street retailer uses RFID in a "track & trace" system for trailer management in their warehouses. It is mainly used for asset visibility.

- ☒ Improved efficiencies in the supply chain, through faster, more accurate and automated exchanges of information between firms. This can lead to improved inventory accuracy and management, better demand and production planning, reduced replenishment times, and so on.

DHL is offering the French fashion industry a way to test item-level RFID tagging of garments in order to help speed the delivery of their products as well as enable shipments to be tracked through the supply chain.

- ☒ Tracking of shipments. RFID allows the tracking of shipments throughout the supply chain, enabling both dispatchers and customers to track the location of goods. Many organisations must also comply with strict regulations regarding the manufacture and sale of restricted goods. RFID improves the traceability of goods in the manufacturing process and can assist in conducting product recalls as a result of safety concerns.

CHEP embeds RFID tags in its pallets, which can then be used by its customers, typically large retailers, to track shipments of goods.

- ☒ Major customer RFID initiatives. Retailers like Tesco and Metro are attempting to drive the implementation of RFID throughout the supply chain. These initiatives are often referred to as "mandates" — though not legally enforceable, they reflect the influence that some large players have on the supply chain.

Metro's rollout of RFID will be deployed throughout the entire logistics process chain. The first phase of the rollout started in November 2004, with around 20 suppliers, gradually extending to about 100 suppliers.

- ☒ Reduced shrinkage/theft. Tags can be attached to high value items to validate their authenticity, or to guard against theft, either within the organisation and its supply chain, or at retail outlets.

House of Fraser is looking at deploying RFID tags on high value items, such as designer sunglasses, to reduce theft.

All of the firms that IDC interviewed use RFID to enhance their supply chain information, though this is not always the primary or initial reason. For example, security and anti-counterfeit motives may prompt some retail firms to adopt RFID early, and adoption may evolve to incorporate supply chain improvements later.

RFID: EXTENDING THE EDGE OF THE NETWORK

RFID technology stretches the boundaries of the network to the very edge of the organisation. It allows data to be stored and modified at an unprecedented level of granularity, providing business intelligence at pinpoint accuracy.

RFID is a network technology. As such, it must be integrated with, as well as extend, an organisation's existing network. The RFID infrastructure layer is only the foundation of an RFID-enabled solution. The success and value of RFID depends on how well companies integrate and enhance their enterprise applications and infrastructure, and how they adapt their business processes to take advantage of real-time supply chain visibility.

RFID is a network technology, and must be integrated with, as well as extend, an organisation's existing network.

Thus an RFID ecosystem can be thought of as having three core layers (figure 1):

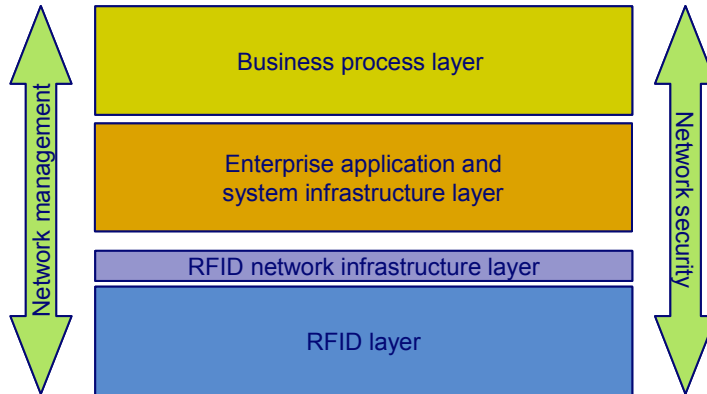
- ☒ RFID layer. The foundation layer, including RFID tags, readers (with their associated antennae), edge servers connected to the readers, RFID middleware managing the flow of data from the edge servers to the enterprise application and system infrastructure layer. Most organisations using RFID today are deploying solutions in the RFID layer.
- ☒ Enterprise application and system infrastructure layer. Database structures, business applications and middleware need to be augmented to handle the potential influx of data created by RFID and work in conjunction with RFID middleware sitting in the RFID layer. Enterprise applications need to be upgraded or redesigned in anticipation of the introduction of real-time supply chain visibility.
- ☒ Business process layer. This is the layer at which competitive advantage will be won or lost, especially in the long term when RFID becomes a commodity. It includes merchandise planning and allocation, store operations, sales and marketing, and so on. This layer should ultimately drive the decision to deploy RFID within, and beyond, an organisation.

In addition to the three core layers, some leading organisations are deploying a specific RFID network infrastructure layer to supplement existing network infrastructure and to provide the dedicated, optimised resources that are required, particularly in large or complex deployments. This intermediary layer supports RFID-related network elements, such as standardised protocols (ISO/IEC RFID standards, 802.11a/b/g etc.), as well as virtual, wireless and wireline LAN configurations.

Embedded throughout the ecosystem is the requirement for network security and management.

FIGURE 1

Layered RFID Ecosystem



Source: IDC, 2005

Extending the Network Boundary Through RFID

Many organisations are starting with RFID pilots within the confines of their own environment, as *localised internal deployments*. The reason for this is simple: it restricts the scope to a manageable limit, allowing learning to occur in a controlled manner. But most organisations implement RFID to facilitate supply chain efficiencies, so extending RFID beyond the organisation is inevitable. Even so, there are some small steps that an organisation can take in venturing outside their own environment.

Example: Metro's initial rollout involves 20 suppliers. Later it will be extended to 100 suppliers, eight central warehouses and 269 retail outlets.

For example, many organisations are implementing RFID in partnership with companies adjacent in the supply chain. These bilateral deployments again allow system testing and experimentation in controlled circumstances. Importantly, though, the value of the pilot to both organisations should increase, as information flowing between the partners improves. At this point, organisations will also seek to embed RFID deeper into their own infrastructure, aiming for short-term *operational efficiencies*.

Example: House of Fraser has partnered with EXEL Logistics, integrating RFID across EXEL's warehouse in Hong Kong with HoF's distribution centre in the UK

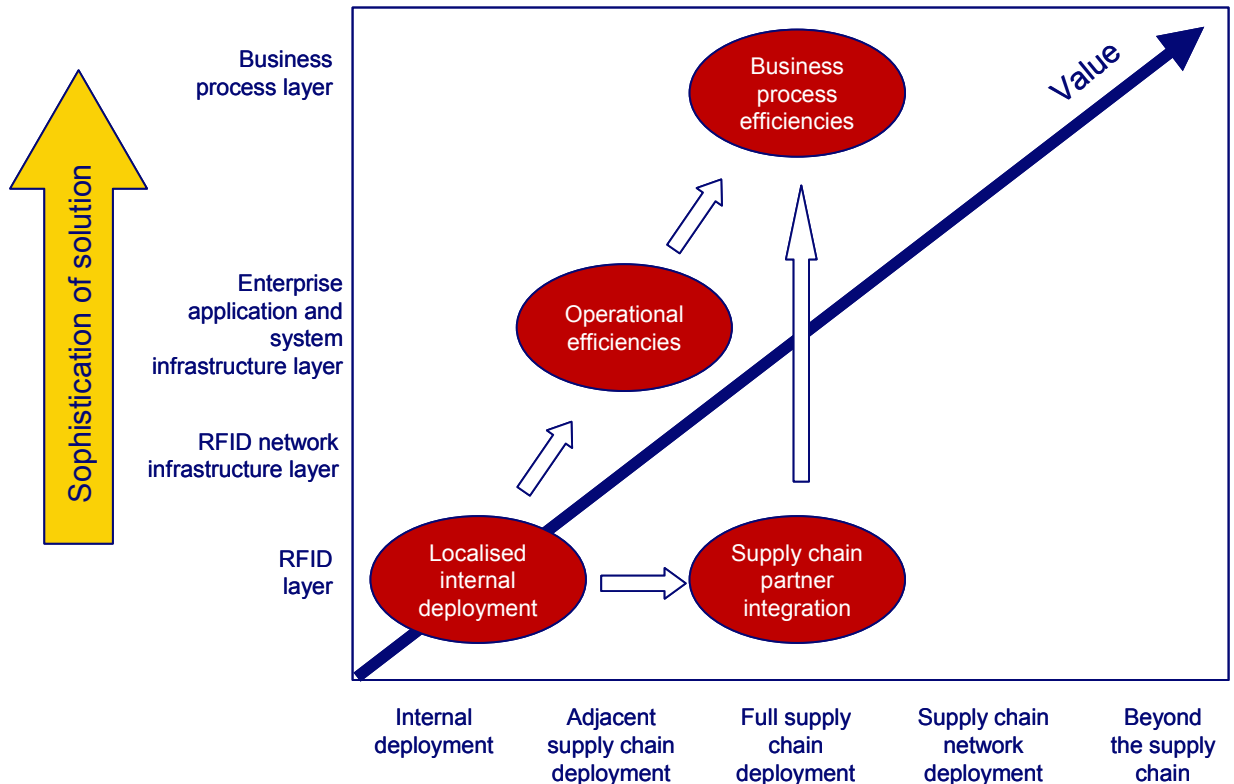
As RFID standards become stable, we will see entire supply chains migrating to RFID, in a phase of *supply chain partner integration*. Organisations will incorporate the improved data flows into improved business intelligence, gaining *business process efficiencies*.

Eventually, networks of supply chains will be interacting. It is even possible that RFID may break away from supply chains to pervade everyday life.

Figure 2 shows how RFID topologies and boundaries interplay, and how the value derived from RFID grows accordingly.

FIGURE 2

Growth in RFID Value



Source: IDC, 2005

WHY RFID AFFECTS THE NETWORK

Radio frequency identification (RFID) tags store information in a compact form factor. It is the size, and subsequent low relative cost, of RFID tags that make them suitable for proliferation in the retail, manufacturing and logistics supply chains. In such environments, the numbers of tagged elements to be tracked can be large, measured in millions of tags. If information from tags is captured frequently, it is imperative to understand how that information is to be used.

Not surprisingly, the ways in which RFID is deployed affects the impact on the network. Since tags store information, which may include location data, not all intelligence need be held in corporate networks and enterprise systems. Exchange of information may be restricted to tags and readers, may be processed by a local server via a LAN, or aggregated and passed on to a distribution centre.

There are two broad types of network impact from RFID:

- ☒ Impact on network traffic, due to the change in information flows through the organisation
- ☒ Impact on network design, including network components as well as other network-connected equipment

The following sections in this paper discuss each of these sources of impact of RFID on the network.

THE IMPACT OF RFID ON NETWORK TRAFFIC

It is often assumed that network impact is dependent largely on the volume of data generated by reading millions of tags. But simply reading tags is not the whole story.

The causes of network traffic impact are threefold. Firstly, the entity on which the tag is located has an influence on network traffic. Tracking at item level generates more data than at pallet level, which creates more traffic than tracking at container level, and so on.

Secondly, the volume of data potentially passed over the network is not just a factor of the number of tags in circulation and the length of an EPC product identifier. The EPCglobal standard contains an object naming standard (ONS) that allows a tag to specify the location (IP address) of product information stored elsewhere on the network. Thus a tag read can generate the sourcing and retrieval of data from anywhere on the network (including supply chain partners). Depending on the demands of the application receiving tag data, retrieval of relevant data may include manufacturer information, customer information, delivery instructions, price, expiry date and so on. This will compound the data volume issue substantially.

Example: A large high street retailer uses a Web-based infrastructure to relay RFID data across the network

Thirdly, a key feature of RFID systems is automated event generation, where the scanning of a tag causes a notification or alert through the system, such as notifying a customer in the change of status of their shipment. These events, while adding the value of traceability and monitoring to the system, add to the volume of data carried over the network.

Addressing these issues is not straightforward. Organisations that expect to generate high data volumes may choose to aggregate information before passing it on through the network, to avoid overloading available bandwidth. Care should also be taken in specifying system-generated events. Pallets and cases may be scanned many times as they are unloaded from a container, carried by forklift truck to a loading bay and loaded onto a truck. Does the customer really need notification for all of these events?

The question is: where should these decisions be made? If the imperative is to manage the amount of data over the network, then it makes sense to manage data volumes at the network level, as close to the RFID edge as possible. Data cleaning/filtering and aggregation is best performed at the point of data capture, embedded in an intelligent network infrastructure. Data volume management, therefore, must be a core part of any RFID system implementation. Keeping data, and decisions, close to the network edge can reduce network traffic, as well as improving inventory control, stock replenishments and theft reduction.

Keeping data and decisions close to the network edge can reduce network traffic

Increased data flow is a function not only of the amount of RFID tags, but also of the rate of exchange of information, either within an organisation or between partners in a supply chain. The optimising of such data flows is critical in RFID deployment and the efficient handling of events.

By locating processing of application events (sometimes termed application layer events) as close as possible to the RFID readers and tags, an RFID system can maintain optimal performance. Intelligent network components not only route events but also interpret their meaning and context in real time, thus ensuring sophisticated processing of events based on their content. This capability also acts as a security mechanism, checking for viruses and other harmful content, and routing infected events into quarantine areas.

It makes further sense to also position storage holding application-related data at the network edge, utilising SAN technology.

THE IMPACT OF RFID ON NETWORK DESIGN

As discussed above, the impact on network traffic, just in terms of volumes, is often understated. But the impact on the network extends beyond traffic to the very network architecture itself.

At the earliest stage of RFID deployment, consideration of network availability and security are important, as well as connectivity between the RFID layer and other parts of the ecosystem. In other words, organisations must pay attention to basic quality of service.

Network Availability

By linking an EPC tag to information held online, the availability of the network becomes central to the RFID application. Critical data required to process a tag read must be retrieved from the appropriate location, whether this is on a local intranet or supply chain extranet. Indeed, some organisations use Internet-based discovery services to publish EPC product information.

Dependence on remote data requires high resilience of the network, possibly above that currently offered with the existing infrastructure.

Security

The exchange of sensitive product data over the network between organisations that may have no direct commercial relationship creates security concerns. The network itself must be secure, logical data access to product information must be authorised (using digital certificates, for example), and physical access to tags, readers and other assets must be controlled.

Equally vulnerable is the network at companies' distribution centres, warehouses, and store rooms, where RFID-tagged cases, pallets, or other items enter into the possession of a company or one of its stores. Unsecured wireless networks present opportunities for eavesdropping on data.

In fact, all the usual security issues apply to RFID, from interception of wireless transmissions to authenticating unknown parties requesting data. These are compounded by the potentially high number of tags and readers, which increases the opportunity for vulnerabilities to be exploited.

Example: Metro applies its existing security software and policies to its RFID deployments.

Specific RFID security issues, such as the accessing of personal data, are being progressively addressed through standards. EPC Gen 2 (ratified in December 2004) features a "kill" command that renders the tag unreadable. But there is no standardised provision for encryption, requiring organisations to add this capability if deemed necessary.

Using intelligent middleware in the network infrastructure layer provides capability to determine the credentials of events and other data flows. It can also provide intelligence to the business process layer, for controlling end-user access to event information.

Storage

With the possible millions of tags and thousands of readers in an RFID system, the prospect of substantial increases in data storage presents significant challenges for a network infrastructure. Storage must be flexible and scalable to grow with the RFID rollout. A storage area network (SAN) solution provides this capability by pooling of networked storage resources, as well as building in a high degree of resilience, security and business continuity to the network infrastructure.

Device Management

RFID deployments potentially involve thousands of readers and millions of tags. Managing such a proliferation of assets demands a device management capability involving the standard features found in all asset management solutions, such as the following:

- Maintaining hardware and software inventories
- Performing software and data distribution
- Managing security configurations
- Enabling remote control for systems diagnostics

RFID device management solutions also include advanced functions that address the unique needs of the environment. These solutions include the following:

- Some automated event systems alert, and even heal, problems automatically. This requirement is a function of the large number of devices in circulation, and the consequentially high effort required in manual device management.
- The ability to manage standards across continents. For example, the recently approved EPC Gen 2 standard will need to be distributed either in new devices or updates to firmware. Differences in bandwidth and radio frequencies between the US and Europe, even within Gen 2, cause further management issues.

- ☒ The ability to incorporate information from tags and readers outside the control of individual organisations. Broad heterogeneity of readers and tags connecting to an extended RFID network is inevitable.
- ☒ Scalability of the solution. As RFID evolves, and incorporates such implementations as sensors (to detect variations in temperature, light, weight, etc.), the number of devices in circulation breaks into the trillions. Because of the internetworking of supply chains and other RFID systems, the number of devices that need to be recognised by a device management solution also increases.
- ☒ Power over Ethernet (PoE) is a strong contender for RFID readers, which work using low wattage DC supplies. Power management is as big an issue as bandwidth management when connecting thousands of devices. Using PoE it is also possible to monitor and control power consumption, which helps prevent the connection and powering of unauthorised devices. Intelligent network switches can limit the power going to the readers to exactly what is required by the reader, so that illicit devices cannot be plugged in.

RFID device management will be an ever-increasing task as the number of RFID tags, readers, printers/encoders and sensors grows. Management extends beyond the simple tracking of devices and includes configuration of devices related to physical locations or even specific business processes. Network-based device management tools can be used to provide data back to the management system itself, keeping device proliferation, movement and usage under control.

Evolving RFID Deployments

All of the considerations outlined above are important for RFID, even in the early stages of deployment. Many organisations are trialing RFID in localised pilots. But scalability of RFID infrastructure is mandatory: it is the nature of RFID to proliferate devices, data volumes and other demands on the network and IT infrastructure, and infrastructure scalability, by definition, implies that it is designed in from the start.

Example: CHEP operates over 200 million wooden pallets worldwide, of which half a million currently have tags. The scope for growth is immense.

Some of our interviewed companies complained about the lack of integration between different suppliers of RFID equipment. It makes sense to approach RFID as an extension of, rather than peripheral to, the enterprise network infrastructure. In this way, issues such as standards and equipment compatibility are addressed at an architectural, rather than device level.

As organisations move out from their internal pilots to broader deployments they take advantage of the planned scalability of RFID infrastructure. This involves extending instances of infrastructure components in a consistent manner, irrespective of their physical location. This is particularly important in distributed operating environments such as retail and logistics, where physical resources (middleware, back-office applications, datacenters, etc.) can be located anywhere.

RFID system expansion is also where automated event generation and event routing and management become fundamental to the premise of RFID. RFID is about asset tracking, and the reporting of exceptions (such as lost or overdue entities). Again, the role of the network is critical here. A core function of any network is the effective and efficient routing of information (data and voice): what better system to route RFID events.

Ultimately, the network and the applications it supports will become integrated, with application-aware networks able to understand messages flowing over the network and automatically invoke security, different routing patterns, and so on. This network nirvana will create automated routing of RFID-related information across the network, dramatically increasing the efficiency and performance of large RFID systems. IP version 6 provides opportunities to embed RFID support within the network protocol layer, thus maximising the integration between RFID and the network handling of RFID-related data flows.

Metro is testing event management notifications where store shelves can indicate when they are nearly empty. The shelf then sends a message to the store manager alerting that the shelves need to be refilled.

CONCLUSION

RFID system expansion is inevitable, as proliferation throughout the supply chain is a core premise for the realisation of system benefits. It is important for organisations to consider the impact on network infrastructure at the beginning of RFID rollout, and to build in scalability from the start. Adjusting the network design retrospectively will be complex and expensive.

RFID technology impacts on an organisation's network infrastructure in two ways: increasing traffic, and impacting the design of the network itself. In fact, traffic is more likely to increase as RFID is rolled out throughout the supply chain. As more and more partners in the supply chain are linked into the system, and more things are tagged, more data is generated and passed throughout the network.

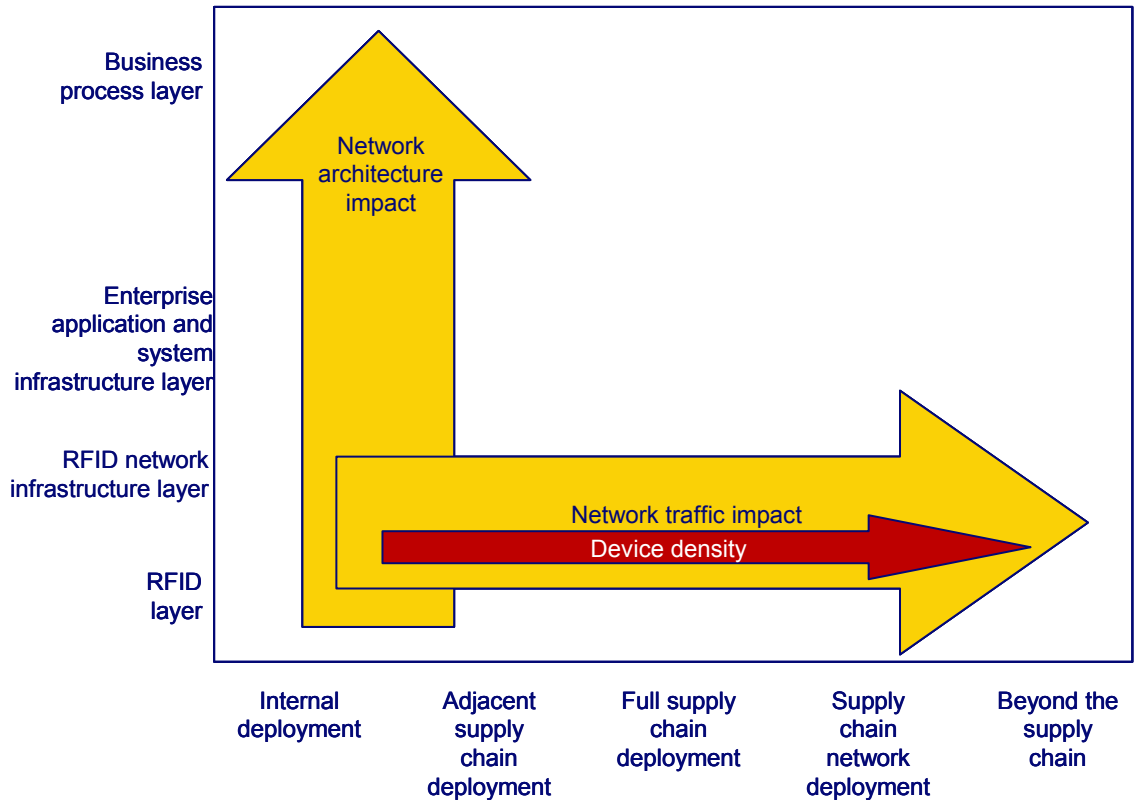
The impact of RFID on network traffic requires the network to be capable of handling the demands of RFID in terms of data volume, increased dependence on availability, and security requirements. Importantly, can RFID be implemented while maintaining network performance for other business operations, such as voice communications and transaction processing?

Similarly, network design is affected primarily by the extent of integration with an organisation's internal environment. Network design is tangibly affected by RFID at the edge, through the addition, provisioning and management of devices, as well as the deployment of SANs, PoE and other network features. This impact increases as soon as an organisation starts to integrate RFID with the rest of its technology infrastructure. When RFID influences and eventually changes business processes, this is where network design is most highly impacted.

These impacts can be plotted against the network topology and boundaries discussed earlier in this paper (Figure 3).

FIGURE 3

Roadmap of Network Impact



Source: IDC, 2005

Figure 3 also shows that, in addition to the increase in impact on network traffic as the RFID system rolls out across the supply chain, the density of devices (readers and printers/encoders) also increases. RFID has a limited reading range (typically centimetres for handhelds, meters for loading bay doors) so potentially hundreds of readers are required in retail, manufacturing and distribution sites in order to provide sufficient reader coverage.

A Call to Action

So given the complexity of RFID evolution and its impact on network design and capacity, what should enterprises do? Figure 4 shows the key issues and priorities for enterprises in each layer of the ecosystem, and depending on the scale of deployment.

In internal deployments, IDC recommends that organisations take the opportunity to plan ahead. Addressing the impact on the network requires action at the network level, and planning a scalable network architecture for RFID at the outset is essential. Scalability also applies to business processes, and organisations should review the prospects for business process improvement.

Planning a scalable network architecture for RFID at the outset is essential.

As RFID is rolled out beyond the organisation's boundaries, it is appropriate to check the infrastructure for any bottlenecks. Testing the capacity of the network while interacting with just a few partners presents a low-risk approach to assessing network impact. As information travels outside the organisation, security becomes a high priority. Any adjustments to infrastructure design should be made before the system extends across the full supply chain.

This is because demand on the network and attached devices soars; as multiple organisations interconnect their RFID infrastructures, the number of devices and tags, as well as the amount of network traffic, rises significantly. Any planned scalability should now be deployed, as service degradation is a key threat. Device density increases substantially, so device management also becomes critical.

To continue to benefit from RFID once commoditisation has occurred requires more sophistication at the business process and infrastructure layers. Application-aware network capability can add substantial value by implementing application logic and routing at the network level, thus increasing efficiency while reducing network traffic.

FIGURE 4

Key Issues and Priorities as RFID Deployment Evolves

Business process layer	Plan business process improvements	Identify business process bottlenecks. Redesign processes to drive RFID deployment	Business information soars. Deploy network intelligence to avoid overload	RFID is commoditised. Seek competitive advantage through intelligent event routing	
Enterprise application and system infrastructure layer	Plan scalability of storage, network capacity and device management.	Identify infrastructure bottlenecks. Extend scalable infrastructure as needed	Bandwidth consumption soars. Maintain QoS of data and voice services	RFID information flows saturate the network. Deploy application-aware network capability	
RFID network infrastructure layer	Plan for proliferation. Consider appropriate RFID standards	Security is a priority. Assures data and physical boundaries	Device density soars. Device management becomes critical	Tags and readers pervade via a universal standard	
RFID layer					
	Internal deployment	Adjacent supply chain deployment	Full supply chain deployment	Supply chain network deployment	Beyond the supply chain

Source: IDC, 2005

LEARN MORE

Related Research

- ☒ *The RFID Ecosystem for the Retail Supply Chain*, (Doc #30311, October 2003)
- ☒ *RFID - A Close Look at the State of Adoption*, (Doc #32399, December 2004)
- ☒ *Worldwide and U.S. RFID Services Competitive Analysis and Leadership Study, 2004: Disruptive Technology in Waiting and Why the Services Value Chain Matters*, (Doc # 32183, November 2004)
- ☒ *RFID: Large Players Shape Up for Battle*, (Doc #SN07L, July 2004)
- ☒ *U.S. RFID for the Retail Supply Chain Spending Forecast and Analysis, 2003-2008*, (Doc #30490, December 2003)

Glossary

EPC: Electronic product code — a globally-unique object identification which is stored on an RFID tag. EPCs are controlled by EPCglobal Inc.

EPC Gen 2: The EPCglobal UHF Generation 2 protocol — a consensus standard developed by more than 60 of the world's leading technology companies. It describes the core capabilities required to meet essential EPC performance needs as set by the end-user community.

RFID: Radio frequency identification — A typical RFID tag consists of a microchip attached to a radio antenna. The chip can store as much as 2 kilobytes of data, such as information about a product or shipment: date of manufacture, destination and sell-by date. A typical reader has one or more antennae that emit radio waves and receive signals back from the tag. The reader then passes the information in digital form to a computer system.

ONS: Object name service — Analogous to the DNS, or domain name service, used to locate information resources on the Internet. ONS uses a standard EPC and maps this to additional data about an object stored on a server connected to the local network or to the Internet.

PoE: Power over Ethernet. PoE eliminates the need to run conventional power cabling to devices on a wired network, such as RFID readers. A single CAT5 Ethernet cable carries both power and data to each device. This allows greater flexibility in the locating of network devices and significantly decreases installation costs.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

For further information regarding this document please contact:

Marketing Department

Tel: +44 (0) 20 8987 7100

Copyright 2005 IDC. Reproduction without written permission is completely forbidden.



IDC is a subsidiary of IDG, one of the world's top information technology media, research and exposition companies.

Visit us on the Web at www.idc.com

To view a list of IDC offices worldwide, visit www.idc.com/offices

IDC is a registered trademark of International Data Group