

EMC PERSPECTIVE



**21st Century Infrastructure
Management: A New Mindset
for Service Providers**

21st Century Infrastructure Management: A New Mindset for Service Providers

Executive summary

The telecoms market is in the midst of upheaval with new technologies, changing business models, and the opening up of opportunities for new competitors and services. The level of complexity, which service providers face in managing networks, applications, and services is growing on a daily basis. Fixed, mobile, managed, and cloud service providers are undergoing organizational, technical and business process change to adapt to what their customers demand in the most rapid, effective, and profitable manner.

In this paper, we take a look at what the changing telecoms landscape means for all players in the market: fixed, mobile, and managed service providers (MSP). In sections 1 and 2, we will take a look at the drivers in the telecoms market and the opportunities for service providers to profit from this new world order. New services are essential for survival and to avoid being relegated to mere “dumb pipes” for each company’s services. Key among these are consumer services, such as IPTV and enterprise services, including cloud computing. In both of these markets, telecoms service providers are positioned to profit as they have the skills and infrastructure in place to deliver high-quality IP-based applications and services.

While the wide uptake of all-IP infrastructures is making these new services possible, they also present service providers with an increasingly complex architecture that makes the silo-based infrastructure management of old too unwieldy and inefficient. With service quality of utmost importance in this consumer-powered age, network management is increasingly important to prevent service providers from losing customers because of poor service experiences.

The battle to remain in control of the infrastructure must also be balanced with the requirement for the customer to see the performance and behavior of the IP applications in real time to protect end-user service performance. An analysis of the network management challenges of modern infrastructures forms the main part of this paper in section 3. This section will also examine the special demands virtualized infrastructures place on managed service providers.

Finally, we offer a solution to this complexity conundrum in section 4. We say that there is only one way to handle this complexity in a cost-efficient manner: with standardized processes and a high grade of automation for operational procedures. For that, service providers need to take a holistic view of network and infrastructure management, by integrating discovery, service assurance, change, and configuration management. This will also allow them to give end users visibility into their service status or track the progress of a fault.

Industry

Telecommunications

Challenge

While the wide uptake of all-IP infrastructures is making new services possible, they also present service providers with an increasingly complex architecture that makes the silo-based infrastructure management of old too unwieldy and inefficient.

Solution

Standardized processes and a high grade of automation for operational procedures supported by the EMC Ionix family of IT management products

1. Market drivers

Lower barriers to market entry for new service providers, advances in technology, innovative business models, and the flexibility of the IP platform are all increasing competition in the telecommunications market. New competitors are emerging from Internet content and VoIP players like Skype, Google, Microsoft®, and Apple. They are commoditizing traditional voice, video, and data services and compelling carriers and managed service providers to seek new sources of revenue.

The disruptive new players are forcing established service providers to become more innovative and nimble when creating and launching new services, and to remodel their underlying infrastructures to stay competitive. In fact, larger enterprises are already demanding that their service providers offer the innovative on-demand services that smaller businesses and consumers are already enjoying via cloud-based delivery models, such as on-demand storage or processing.

One of the most important technology drivers is the emergence and wide acceptance of IP-based service platforms, which cost about 10 percent of their circuit-switched counterparts, and make it easier to create new services. They also enable service providers to compete more effectively against one another. For example, voice services have seen tremendous pricing pressures due to all of the options now available to communicate or make phone calls. We have seen WiFi phones, VoIP, Internet calling, and even instant and text messaging all become substitutes for the traditional phone call.

Consumer demand

Changing consumer attitudes have put pressure on telcos to provide more tailored or customized services. This affects everything from communications devices, to features, to service bundles, to pricing models. Some examples include à la carte channel subscriptions where users choose and pay for only those channels they want to watch rather than pay for the entire bundle of channels. In the wireless space, users want to customize the content and home screens on their phones so they can quickly and easily access music, video, news, applications, or other phone features.

IP helps service providers meet consumer demand for services that contain a more personalized element, including mobile multimedia services, productivity tools, and self-care web portals.

There has also been a massive growth in user-generated content from consumer blogging, social networking, and video sharing. This growth in content is increasing the demand for higher bandwidth, and leading to an increase in data traffic, thereby making storage and network capacity planning more complex—and increasing the costs for the service provider. Further increasing the challenges for service providers, the costs of carrying this slew of user-generated content across the network has not been matched by increased revenues.

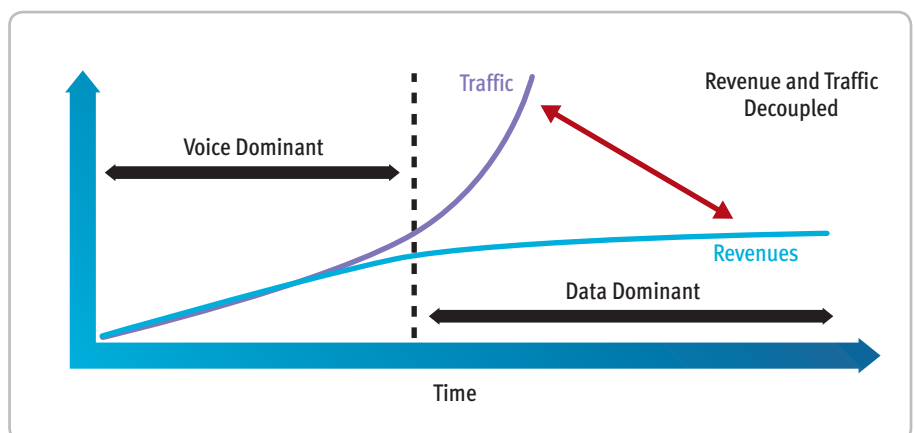


Figure: The gap between traffic and revenue

Pressure on budgets

While new technologies that support compelling services proliferate, such as LTE, femtocells, new smart phones, fiber optic networks, Metro Ethernet, and microwave for mobile backhaul, service providers are finding that their operations are becoming increasingly more capital intensive as network build-outs and upgrades become vital to creating revenue from the network.

To counter this, they are looking to third-party outsourcers and system integrators to manage portions of their IT and network infrastructures, and turn what used to be a one-time lump capital outlay into a recurring monthly operating expense that requires less up-front investment. However, as an exception to this rule, mobile operators are starting to invest in their own backhaul networks to reduce operational costs and their dependence on traditional carriers. Vodafone Germany, for example, has reportedly saved in the region of €60 million in operational expenditure (OPEX) savings according to *European Communications* magazine.

Finally, regulatory uncertainty continues to disrupt the market. Even though regulators have taken a hands-off approach to the Internet, they have been slow to allow carriers to create a tiered-Internet. Additionally, more regulators are requiring telcos to retain and protect customer data records for long periods of time, with the additional burden of being able to retrieve records within a short timeframe. Ultimately, carriers are struggling to make investment decisions when there is a chance that regulation will not allow them to recoup their investments.

2. Trends and opportunities for service providers

Virtually all service providers are looking for opportunities that prevent them from being consigned to being a “dumb pipe.” They are concerned that simply supplying access to services relegates them in the value chain, while the new entrants and “over the top” competitors profit from content, advertising revenues, and closer subscriber relationships.

New technologies, services

New technologies and operational processes often hold the key to becoming more effective in the marketplace. For example, service providers can integrate new networks including LTE and 4G, femtocells, WiFi and WiMAX, and metropolitan fiber to change the economics of service delivery.

New technologies and processes such as virtualization and expanded network reach can also help service providers adapt to new service usage and billing models. These include cloud computing with Software as a Service (SaaS) and Infrastructure as a Service (IaaS), fixed/mobile convergence, unified communications, pre- and post-paid convergence, micropayments, borderless roaming, and realtime subscriber interactivity. Service providers then need to be able to monitor and charge for service usage in real time to properly monetize their networks and enforce fair usage policies to make this successful.

IPTV, IP Telephony

With the ever-increasing consumer demand for next-generation communications services, IPTV is a key opportunity for service providers. When it comes to launching next-generation TV services, fixed and mobile service providers can provide greater competition to cable operators who have broadened their portfolios to compete using mobility services. Fixed and mobile service providers can capture market share if they form new content partnerships, distribution models, and tariffs.

Most multi-system cable operators (MSO) already have an infrastructure in place offering superior integrated services to their customers over broadband connections with 100 Mbps bandwidth capacity. Part of that strategy is the next-generation TV platform that allows customers to watch TV everywhere, with every device, and new quality standards like HDTV and 3DTV.

Customarily, the main telco revenue stream has come from traditional voice services. The popularity of VoIP has led to incredible data traffic growth in carrier networks which stretches their actual infrastructure almost to its limits. But instead of focusing on limiting the potential cannibalization of circuit-switched voice revenues, service providers should embrace VoIP services and offer choices to their subscriber base about how they access and use them.

There is also an opportunity to develop a greener approach to providing services by utilizing new technologies. These include the Smart Grid, deriving power from alternative sources, greener data centers, recycled devices, and launching machine-to-machine (M2M) services that use the cellular network to provide more cost-effective remote access to data information from equipment in the field including cars, vending machines, and even municipal street lighting.

Cloud computing

Finally, cloud computing is a major opportunity for all service providers to increase their service portfolios. For example, fixed and mobile service providers can use cloud computing to move away from a pure bandwidth connectivity business, and managed service providers can offer more flexible and scalable services. Cloud computing gives service providers the ability to develop new service delivery models that match demands from the business community, and applications which can be served up over any access network, in a secure and easy-to-use manner, that are optimized for mobility.

Businesses, which gain a productivity or customer service advantage over competitors from using cloud computing, will likely adapt their business processes to it for the long term. Because cloud computing allows service providers to improve infrastructure utilization and cut power consumption, it improves the economics for both customers and service providers.

Many service providers already have the key components in place: the network infrastructure, relationship with enterprises, and the billing and roaming knowledge that will play an essential role in cloud business models. Predictions for the cloud computing market vary widely. At the conservative end, IDC predicts the market will be worth \$44 billion in 2013, but a number of other analysts have pegged the market much higher. This variation in market sizing is partly due to the difficulty of defining what cloud computing represents, but there is little doubt that there is plenty of market potential for software, platform, and infrastructure as a service.

For all of these opportunities, improved customer experience in service quality, service offerings, and customization is key for service providers to retain existing customers and attract new patrons.

3. Common challenges for players in the telecoms market

In this section, we will look at the challenges facing all service providers in the telecoms market: fixed, mobile, cloud, and managed service providers. The first part covers generic challenges affecting all market participants; while the second part focuses on the additional challenges facing managed and cloud service providers.

New services are essential to help all service providers overcome shrinking revenues and compete effectively; telcos, in particular, need to look to new services to bolster their legacy network income. However, launching new services is a resource-intensive activity and network operations centers (NOC) have to balance the business demand for new services with their own shrinking budgets. For example, there is a major opportunity for telcos to sell managed security services along with network connectivity to their customers' branch sites where there are few in-house IT or security skills.

Unfortunately, these opportunities come at a price. The problem is one of complexity: as the network has become more dynamic, service providers have seen their management challenges increase exponentially. There are more devices, more vendors, and more technologies to manage. Instead of developing new products, the NOC team spends all its time fire-fighting network problems. In fact in our experience working with operators, around 70 percent of budgets are spent on maintenance and only 30 percent on launching new services.

These budgetary constraints are putting pressure on both CAPEX and OPEX spending with cutting the latter particularly important because it accounts for the majority of the total costs over the lifetime of the equipment. However, it can be very dangerous to cut operational costs across the board, indiscriminately, as it can negatively impact quality of service. With customer acquisition costs in telecoms remaining high, this could be a very risky strategy.

The move to IP

Although IP service platforms have opened up many opportunities for service providers, they are also partly responsible for these increased management challenges and operational costs. Because IP is a more open network technology, controlling how devices connect over a variety of wired and wireless interfaces is more difficult. It introduces greater complexity into the way the network and service infrastructures are managed, because they impose a vast number of variables on old system architectures that make discovery and mapping, security, change management, performance, troubleshooting and resolution, and the whole customer order-to-cash cycle much more challenging.

To benefit from new services that use a common IP infrastructure, such as data services, mobile e-mail, browsing, and location services, along with voice and SMS, service providers also need to break free from the silos that have built up organically over the years. In the past, each service had a separate network infrastructure which was managed as a separate entity within the service provider, which meant that there was a very direct link between infrastructure management and service management. However, these new services need to work across silos, and demand a unified management platform encompassing infrastructure and services.

In addition, with the move toward all-IP networks regardless of service type comes the opportunity for operators to converge fixed and mobile traffic onto a single backbone. This allows them to drive down costs and offer innovative services mixing fixed and mobile connectivity. Again, this drives the requirement for service-centric management capability, and the ability to manage multiple device types in the IP/Ethernet technology space.

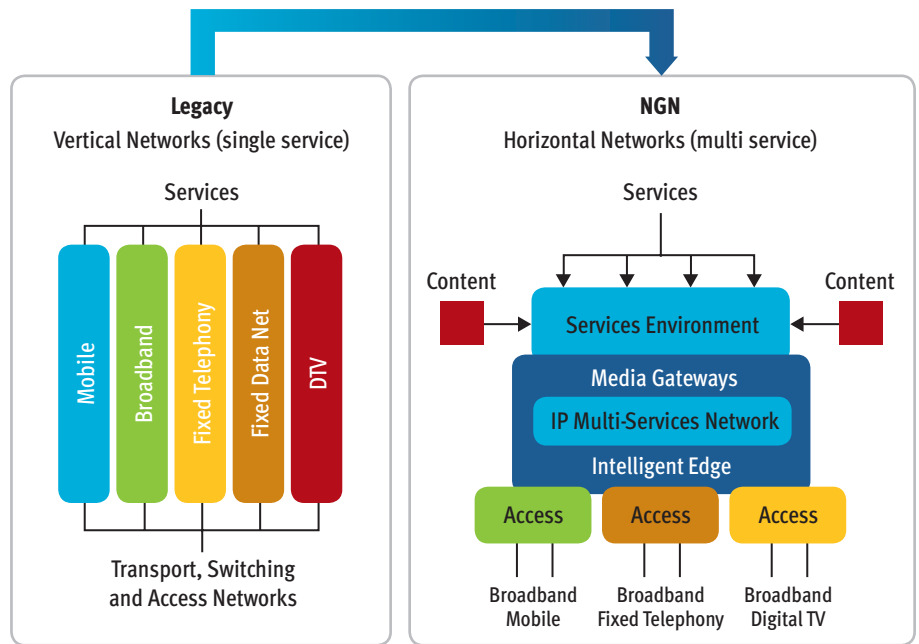


Figure: The network evolution

Limitations of manual processes

With service quality at the top of the agenda, dealing effectively with faults is paramount. However the traditional approach of identifying infrastructure problems using a manual or semi-automatic process no longer is viable in modern complex networks. Look at the mean-time-to-repair (MTTR) service level that most service providers have in place. The bulk of this time is taken up by locating the actual problem. Fixing it may be as simple as changing a hard disk drive or rebooting the server. The real work is identifying the root-cause problem in a sea of alarms within the network operations center.

With network equipment dependent on other components within the network, a single fault can spark a whole tide of red alarms. The challenge is knowing which one is the original alarm and event, and which alarms are consequent alarms. To get there, the NOC might need to go through a cycle of evaluation steps until it identifies the original root cause, or use tools which rely on manually created rules. The problem with the latter is the impact of changing relationships in a highly dynamic environment. For example, if equipment is moved, deployed, or taken out, any change in the topology means that the rules defining a certain combination of alarms (which the NOC uses to identify a root cause) may no longer be valid.

In the wider context, service management continues to be a challenge for how service providers deal with their customers. For example, in most cases telcos will use eTOM to manage their services and networks. Their enterprise customers on the other hand will use ITIL to manage their own infrastructure. This gap between service management approaches needs to be closed to make service management more transparent to customers. To that end, many service providers are adopting ITIL to match the language and approach that their customers are using.

Skills shortage

Service providers also sometimes suffer from a skills shortage in IP fault handling. Many in the NOC come from a telecoms background, and need to adjust their working practices to suit the more dynamic IP world. In the past, the transport network for mobile or fixed services was ATM- or TDM-based, but the toolsets for these environments no longer work, and NOC staff find themselves having to manually set up rules for troubleshooting the network. They are fighting a losing battle, and it can take them weeks or months to come up with a correlation scenario that links a sequence of alarms to a root cause.

Manual processes also leave companies open to risk because much of the information is stored in the mind of the best workers. By automating processes, it's possible to capture all of this tribal knowledge and reduce risk. In addition, solving difficult problems is often left to the most skilled staff, which distracts them from revenue-generating activities such as deploying new services. Automation means that once the processes are created, the most skilled staff can be assigned to strategic activities.

Dealing with misconfiguration

With today's resilient networks, one of the major reasons for outages is misconfiguration. Perhaps a technician has made a change to a piece of network equipment that inadvertently caused something else to fail, or perhaps they have simply pressed the wrong button and created an invalid configuration that creates a local problem. Problems such as these can be prevented by proper governance, such as defining who can change what, and recording the actions they have taken so that any changes that have caused problems can be reversed.

It is important to keep on top of configuration to meet internal standards and regulatory requirements. If someone makes a change that affects a security regulation, such as the Payment Card Industry Data Security Standard (PCI DSS), it can place the organization at substantial risk. To prevent this, it is essential to monitor in real time to ensure that the configuration is always compliant. Additionally, with the increasing proliferation of different regulations worldwide, keeping on top of their different requirements is proving to be a headache for many operators. This is particularly a problem for global operators who will have to comply with a multitude of local and global regulations.

Fear of the unknown

One of the biggest barriers for service innovation is the organizational fear of what could go wrong. There is often a battle between the business, which wants to develop innovative services, and the IT department, which wants to ensure that they remain in control of the environment. Automating complex network management will help organizations keep control of their environment, and modelling tools will give them the ability to see what will happen when new services are launched. This gives the IT department the confidence that they can launch and support new services, enabling the business to be more agile and innovative.

To gain competitive advantage from new services such as IPTV, service providers need to deploy and use a greater variety of equipment. To further complicate matters, service providers will also have to manage equipment across various layers—from optical, to IP/MPLS and its control plane, up to the application and services. Having visibility across all layers is crucial. Otherwise, a widget that has been unplugged in the network could well look like an application problem, rather than an issue with the physical layer.

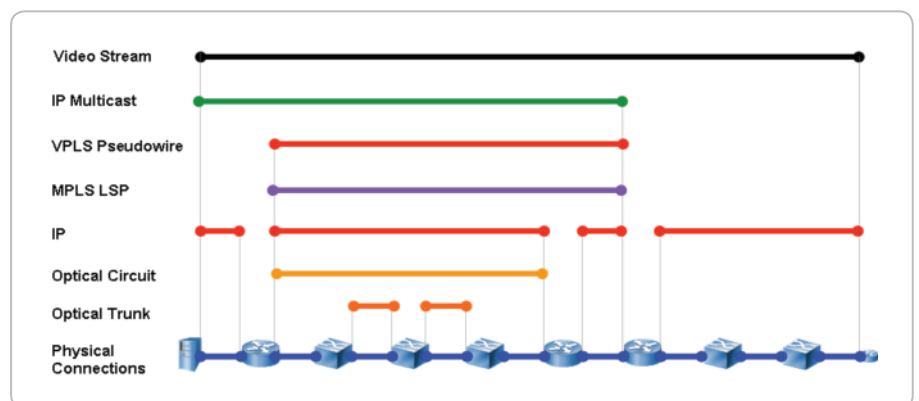


Figure: The complexity of layered technologies for IPTV

For example, if an optical cable breaks, this will generate alarms because the transceivers will no longer see each other. On top of this will be an IP WAN circuit, which can no longer communicate, and an MPLS hop that is blocked. Ultimately this will impact VPN and IPTV services, and the challenge for service providers is to locate the original problem.

Specific MSP challenges

Most of the challenges above are common to all service providers, but managed service providers (MSP) who offer more than just connectivity-related services to their customers face a number of additional challenges. For example, how does an MSP deal with a help desk call relating to poor application response time? Although most users will blame the network, the cause of poor response time could also be a faulty server or overloaded database. It's therefore essential to have visibility over all of these silos and possibly offer a dashboard view to the CIO to show the overall health of the entire environment.

The application infrastructure provides an additional element of complexity for MSPs, and this is exacerbated by the increasing use of virtualization. Although virtualization helps managed service providers deliver new services at attractive price points by sharing infrastructure more efficiently, it also creates a number of complexities that directly impact infrastructure management. However, maintenance and troubleshooting the performance or failure of applications in a virtual environment is challenging since there are a large number of applications, each in their own virtual environment, on any number of servers across multiple data centers.

Keeping track of all of the relationships between physical and virtualized components is critical to manage the infrastructure. For example, if a physical machine goes down, the MSP needs to know which applications are affected. Identifying the root cause of problems across physical and virtualized environments is reported by analysts to be one of the key challenges. The infrastructure management tool, therefore, will need to cope with all the moves, adds, and changes that are part and parcel of virtualization.

There is another problem to which service providers need to pay attention in virtualized and cloud computing environments, and that is "virtual data center sprawl." Because it is so easy to set up virtual machines, there is a danger that you could end up with rogue machines all over, not know where they all are, or if they are duplicating effort. It's therefore essential to have a workflow in place, so that virtual machines are formally requested, and a discovery tool that can locate and identify any rogue machines.

Addressing onboarding time

One of the biggest uncertainties for managed services is onboarding, which is the time it takes to identify all of the customer's equipment and services that the managed service provider is taking over. Typically an MSP would carry out a lengthy due diligence process to assess what equipment is on the customer's premises, and manually set up rules for each device. This often involves the service provider going through the customer's entire infrastructure with a clipboard to see what is where, which is both expensive and inaccurate.

The ultimate goal is to get the customer onto standard platforms so that they can realize return on investment on the contract as quickly as possible. As systems become more complex, this onboarding manual process is posing a serious challenge to MSPs' profitability. Being able to easily discover the elements of the customer's infrastructure is essential to give an MSP better confidence in the price they are offering, and get ahead of the implementation curve. By eliminating the uncertainty inherent in a traditional due diligence purpose, an MSP can eliminate the risk element in the price, and offer a more competitive service.

What this shows is that to benefit from new services, and cut operational and capital costs, service providers need to get control of their network and application infrastructure. The old silo-based management approach worked for smaller telecoms' focused environments, but larger IP-based environments are simply too complex for manual techniques to work.

4. Solving the challenges

The way service providers achieve these objectives is to reduce the number of vertical service provision silos in the network, and pool new service delivery resources. Building an integrated, horizontal, multi-service infrastructure will bring new cost efficiencies. Such a network will benefit from a single, overarching service management dashboard that provides an operational overview and allows service providers to rapidly maximize the performance of their infrastructure, and meet new customer needs rapidly, flexibly, economically, and effectively.

By eliminating silos, it is also easier to build cloud computing services such as Infrastructure-as-a-Service. It will allow service providers to combine the various components of the infrastructure such as storage, processing, and network, into self-contained pools of resources that can be deployed and managed directly. They can then layer the operating system and applications on top of these modules to enable easy application mobility and virtualization.

Getting there requires a change in how service providers manage their networks. Crucially, management modules need to be fully integrated and automated. For example, linking to the discovery and change management information will allow faults to be quickly identified. The EMC® Ionix® family of IT management solutions accomplishes this by integrating discovery and mapping; change, configuration, and compliance; and service assurance.

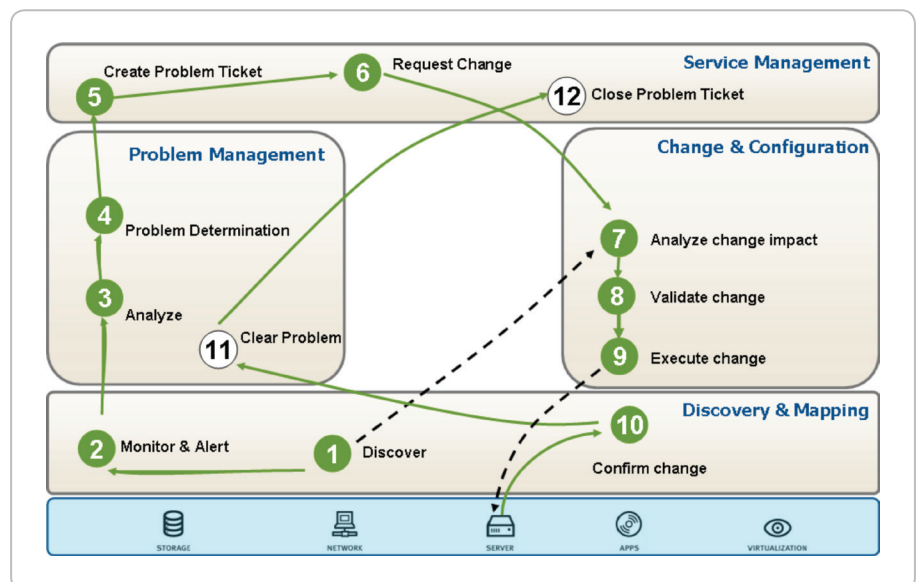


Figure: EMC Ionix - An integrated and linked solution

Automated discovery and mapping is the starting point of the EMC Ionix solution. This populates the ITIL-aligned configuration management database (CMDB) with all of the infrastructure components, including networks, applications, servers, and storage—even virtualized components. It determines the relationship between the assets, such as what runs on which device, and undertakes deduplication.

Change and configuration management is a critical management element, as many faults are caused by configuration errors, as described earlier. The solution enforces company IT policy and provides audit trails for compliance. It also allows for automated validation so that operators know whether their changes meet the company policy. This is crucial for both governance and regulatory compliance.

The service assurance part of the solution is the root cause analysis tool, which undertakes automated fault management and impact analysis. It allows service providers to pinpoint infrastructure immediately across multiple silos. Service assurance is tightly integrated with the discovery tool because it needs to have that relationship to carry out the root cause analysis. Fault management also synchronizes with change management so that any misconfigurations causing problems can be rolled back.

The key business benefits of the EMC Ionix integrated approach include:

- **Eliminating errors**—Automation allows service providers to remove the manual process from their day-to-day activities as they are both error-prone and time-consuming. It will help them eliminate the cost of manually making the relationships between components on the network and the entire service infrastructure, including servers, applications, and storage. This becomes even more important within a growing and highly dynamic infrastructure. Automation can save up to 70 percent of the time isolating problems, and these resources can then be redeployed from fire-fighting to supporting the business.
- **Accelerating infrastructure management**—By automating infrastructure discovery and problem identification, service providers can reduce the length of many management tasks by up to 90 percent. Having a holistic approach to discovery, configuration management, and fault management dramatically speeds up, the tasks of finding and fixing problems within the infrastructure. By being able to execute day-by-day changes on the infrastructure, service providers are also able to deliver new services much more quickly and easily.
- **Optimizing infrastructure**—Service providers are able to optimize their infrastructures by avoiding unnecessary outages and service downtime due to misconfigurations and unplanned changes in their environment. Manual change management causes 85 percent of problems within the infrastructure, so it is essential to prevent configuration errors, such as mistyping, or interoperability issues by validating changes before execution. In addition, Ionix allows them to run “what-if” scenarios to understand what impact a particular configuration changes might have on the infrastructure.
- **Consolidating silos and tools**—By having a management platform that can work across silos, service providers are able to consolidate toolsets for server, network, storage, and application configurations to avoid finger-pointing and a swivel-chair management style. Proactive fault management allows benchmarking of normal network behavior so that action can be taken if it deviates from the norm. In addition, the information will be useful to help different entities within the service provider collaborate together, see their impact on each other, and make support handover easier.
- **Complying with internal and external regulations**—Automated configuration checking will allow the service provider to ensure that their infrastructure is in compliance with both their own IT policies and with regulations such as PCI, HIPAA, and SOX. It will allow them to improve security by having automatic policy compliance, such as enforced password changes, and run regular audits on the fly to prove compliance.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

To learn how EMC products, services, and solutions help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com.