Bringing Better Business Value to Mergers and Acquisitions

Performing IT due diligence is a critical step to ensure the success of mergers, acquisitions and divestitures

A publication of Lumeta Corporation
www.lumeta.com

Drivers for Mergers and Acquisitions

In today's fast-paced global economy, mergers and acquisitions (M&A) are a common strategic business practice that has seen a resurgence in recent years. M&A events occur for a number of reasons, such as increasing valuable market share, adding technology capabilities, gaining an advantage over competitors, and enhancing brand value. In this M&A culture, businesses place an enormous amount of pressure on IT to deliver the large volume of required network changes on time and within budget. These pressures often lead IT managers to make decisions without all the facts, resulting in actions that impact the network's infrastructure, availability, security, and compliance.

Key Factors

M&A activities add new management issues to already complex networks. Successfully completing a merger or acquisition requires that a number of key technology issues be taken into account which if not addressed from the start could jeopardize the success of the M&A activity.

IT managers need to consider the costs of restructuring the network to accommodate this activity. Often, redundancy is the most prevalent factor when merging different networks. In addition to dealing with issues like duplicate facilities, however, IT managers must also eliminate outdated assets; consolidate current assets, applications and services; handle third-party or portal connections; and more.

Many acquisitions or mergers require organizations to provide detailed documentation of network assets quickly, sometimes in a hostile situation. It can therefore be difficult to depend on the quality and accuracy of the documentation received from the merged or acquired organization.

How, then, should a company validate the information received and eliminate potential risks associated with M&A activity? It can be nearly impossible, using manual means, to be absolutely certain that the acquired or merged organization has no insecure public or private network connections, such as cloud instances or virtual machines that can potentially lead to the exposure of core and critical assets to hackers or viruses. How can a business examine the acquired or merged organization's network, assets and associated risks and truly prove its network is secure before the M&A activity has been completed?

Raising the Business Value of M&A through Better IT Due Diligence

Performing IT due diligence is a critical step to ensure the success of the merged network and directly contributes to its performance. A detailed examination of the state of the infrastructure can help ensure that strategic decisions are based on rational analysis and not on anecdotal data, hearsay, or “guesstimates.”

Such upfront, unbiased initiatives can also help avoid costly delays and network breakages caused by surprises that invariably crop up weeks or even months later, making post-merger integration difficult and also generating cost overruns.

Due diligence activities typically focus on business and financial issues. Even so, many organizations fail to look closely enough at the effort needed to join two complex networks. As a result, companies often enter into M&A transactions with a greater risk profile than they originally estimated.

Common mistakes made include:

- Performing a limited IT assessment – Companies often make the assumption that taking a cross-section of an enterprise network will provide a sufficient model for the entire enterprise.

- Focusing on “getting the deal done” – Organizations often lose sight of how things will look after the first company-to-company connections are made. This lack of comprehensive understanding occurs when the organization limits the scope of IT due diligence to the “as-is” state of the merging companies, instead of the future state envisioned by the merger.

- Failing to understand what the infrastructure actually looks like versus what was envisioned –Companies often fail to migrate and optimize networks to a converged network from the outset. The result is that within a short time, yet another costly project will be required in order to clean up legacy systems and connections that still exist in the organization.

Improperly planned M&A network activities can create project delays and huge cost overruns, often putting the entire enterprise at risk. As organizations utilize the IT infrastructure to improve business performance, it is incumbent upon them to tackle integration issues upfront in order to keep costs low and performance high. These efforts include increasing the scope of their M&A due diligence to include a full discovery of both organizations’ networks to find overlaps in assets and connectivity.

The main network cost benefits of M&A activity are realized when assets or network devices are standardized, maintenance and support is consolidated, and IT risks are minimized effectively to avoid issues such as:

- Clash of address space
- Connectivity bypassing the security fabric of the enterprise because of culture and policy differences
- Multiple servers doing the same job

How to improve business value in Mergers & Acquisitions

Pre-merger – Stage 1
- Baseline the network

During Merger – Stage 2
- Continue streamlining the scanning process
- Monitor and pinpoint baseline deviations
- Reproduce new visual network maps
- Monitor risks

Post-merger – Stage 3
- Compare before and after network maps
- Continue monitoring network changes
- Continue monitoring ongoing risks
- Provide ongoing audit and measurements

The Lumeta Solution

Lumeta® IPsonar® provides a crystal clear analytical view of the entire corporate network.

Even in the best run networks, Lumeta has found that administrators are unaware of as much as 20% of their actual network assets. This lack of visibility is severe enough to hamper initiatives such as:

- New application deployments
- Vulnerability and incident response programs
- M&A activities and network consolidation
- Security policy compliance and audit programs
- Current as well as planned operating and infrastructure updates

IPsonar is the only solution that can discover what organizations do not know and cannot know through manual means. Originally developed to map the entire Internet, its sensors detect all access points without requiring that it be programmed to look within preset fields.

The solution is backed by the **Lumeta Network Index** Score Card, which offers accurate before and after risk assessment figures related to infrastructure changes. The Lumeta Network Index also provides audit measurements and risk factors for baselining.

The Lumeta Network Index:

- Gathers information from IPsonar scan data
- Provides a scorecard for common network issues based on industry research and best practices
- Addresses four major risk categories
    - Network topology
    - Network address space
    - Network leak paths discovery
    - Device fingerprints
- Defines prioritized and proactive risk avoidance automatically calculated and prioritized based on scan
    - Higher risk scores indicate actionable items
- Helps mitigate the top issues for best ROI results

This baseline can be presented at any time to the corporate board for ongoing understanding of the changing infrastructure needs, and can be sent to auditors for compliance reasons, to different geographical regions to compare network management and discovery capabilities, to subsidiary divisions to keep them competitively on their toes, and to outsourcers or merging or acquiring businesses for business transition identification checks.

Pre-merger – Baselining the Network

The first and most important step before beginning the network aspect of M&A activity is to scan both organizations' entire networks. This, in itself, is a huge burden on many network managers, as they are required to accurately gather material quickly and accurately. IPsonar can automatically scan both networks, saving time, effort, and cost compared to finding different vendors to deliver various requirements.

The most sensible starting point in the evaluation of the integration between organizations is scanning and understanding the core services on which the entire business depends for continuity. This may include, but not be limited to, all IP services such as:

- LAN and WAN connectivity
- Public, Private & Hybrid Clouds
- Virtual Machines
- IT security
- Internet/intranet access
- Voice services
- Videoconferencing
- Email
- Cross-platform sharing
- Desktop applications
- Remote access

During the Merger – Providing Network Situational Awareness

In order to assure a smooth network merge, organizations must discover the type of information being communicated across a network, map the network architecture, review security controls and vulnerabilities, and thoroughly evaluate risk management strategies on an ongoing basis. Thus, they can more easily implement, validate, and maintain appropriate standards.

IPsonar, a Lumeta Network Situational Awareness solution, complements system and data security efforts to round out M&A Information Assurance (IA) processes. Network Situational Awareness addresses the dangerous gaps produced in IA processes when rapid network change causes organizational policy and network defense configuration to become misaligned. Lack of network visibility can seriously hamper network change and security initiatives, having a negative impact on availability of resources or creating unintended security risks. The best way to eliminate serious risk to the integrity and availability of systems and data is through the complete visibility of connectivity that Network Situational Awareness inherently provides.

Using IPsonar, organizations can:

- Continue streamlining the scanning process
- Monitor and pinpoint baseline deviations
- Reproduce new visual network maps
- Monitor risks

The network management and intelligence solution provides features for network discovery, host discovery, leak path discovery, and device fingerprint discovery - finding routes and routers, hosts, servers, unauthorized connections or hosts, and perimeter leak paths.

Network Discovery

Given the frequency of change in large networks and the error prone way in which changes are made, organizations often struggle to ensure that all network assets are under management. Unmanaged assets increase the risk of intrusion and service outages.

IPsonar's Network Discovery:

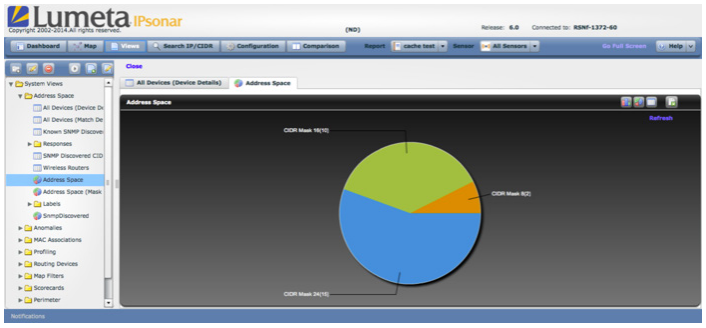
- Applies multi-protocol discovery to penetrate deep into the network, identifying forwarding and filtering devices
- Traces the path of data through the network, indicating whether assets communicate properly
- Flags "stealth" assets that do not respond to queries, pinpointing resources that may not be under management
- Isolates the impact of firewall and router access control lists (ACLs), assuring they are operating in compliance with policies
- Provides a comprehensive, route-based network topology from an application connectivity perspective

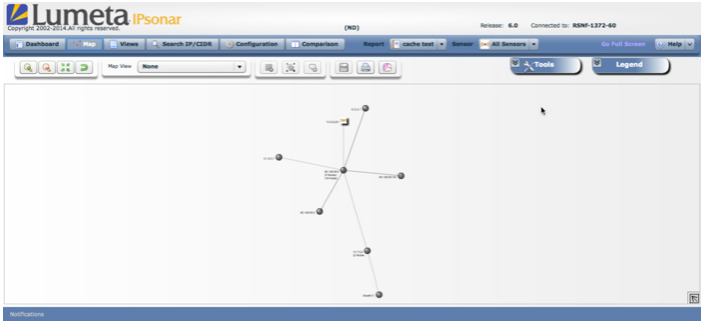
Host Discovery

In a sense, the network is a collection of IP addresses which IT organizations are responsible for securing. Yet unknown IP addresses exist in every large network, often undiscovered until they cause an outage, breach, or audit issue.

IPsonar detects all known and previously unknown network addresses, helping IT executives align their areas of visibility with their areas of responsibility. IPsonar's Host Discovery:

- Conducts a census of all IP addresses using multi-protocol discovery, identifying the true perimeter of the network
- Flags previously unknown addresses – those not recognized by official network inventories – for remediation
- Enables organizations to harden defenses around their network perimeters and secure zones to enforce policies





Leak Path Discovery

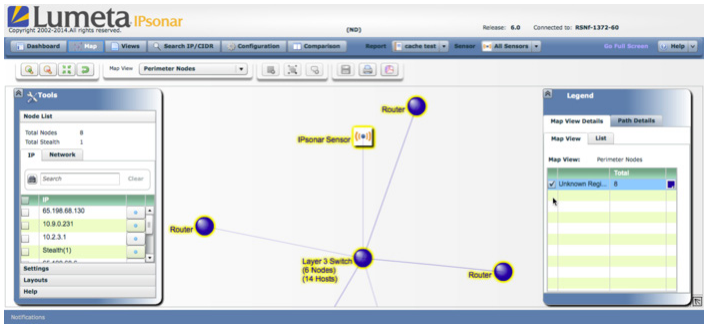
Leak Path Discovery is the process of detecting unauthorized inbound or outbound connectivity to the Internet or sub-networks.

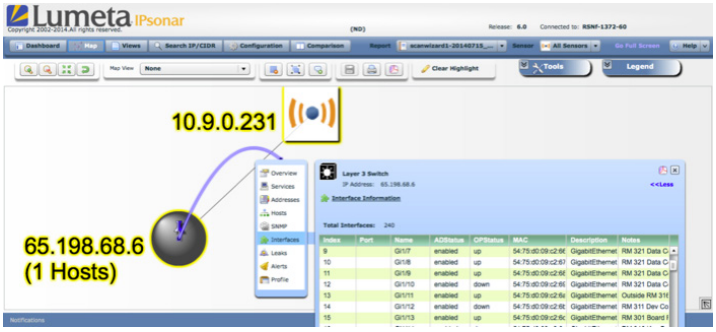
The more complex a network, the more likely it is that unauthorized leak paths exist. Defending information and operations from threats requires that IT organizations proactively identify these leak paths, such as unsecured routers exposed to the Internet or open links to former business partners.

IPsonar reveals all unauthorized connections, identifying whether access is outbound, inbound, or both. IPsonar's Leak Path Discovery:

- Pinpoints forwarding and filtering devices, enabling IT staff to ensure that these resources are in compliance with security policies
- Flags inbound and outbound connectivity to secure zones, such as those developed to protect customer data or carry sensitive communications
- Identifies resources a "hop" beyond the network, showing executives to which organizations they are connected
- Spots hard to find leak paths such as unauthorized cable/DSL routers, multi-homed servers, and NAT/PAT proxies that covertly forward network traffic

Leak Path Discovery also highlights unknown connections into other organizations – such as legacy divestiture connectivity. Once a divestiture is completed, an organization should verify that the divested network assets are actually disconnected.





Case Study: Fortune 500 Corporation Identifies Active Divested Company Connections in Enterprise Network

Business Challenge:
One of the largest oilfield services companies was implementing a major divestiture of their construction and project management subsidiary. The client's major focus was to prevent any business disruptions that could occur from the network segmentation of the main company and the spinoff division. The combined network is over 300,000 IP addresses and many business processes are run across the combined networks.

Solution:
Stage Lumeta ran an initial Lumeta Network Assessment service over a 90-day time frame. With the use of Lumeta's IPsonar product, which includes interactive mapping and visualization, a complete and thorough understanding of this inter-connectivity and touch points was easily uncovered.

Results:
This visualization and database results included:

- Routers with shared interfaces; interfaces still up and running
- Multiple ingress/egress points into both enterprises
- Leak paths uncovered while verifying the divesture
- Multiple devices identified with residual community strings
- Multiple Internet connections
- Shared network addressing schemes needing remediation

The results provided a clear roadmap for the client in its effort to become completely divested of its subsidiary.

Device Fingerprinting

Assessing risk requires more than a census of assets and their interdependencies. To determine whether assets are non-compliant or vulnerable to a specific threat, IT organizations must understand their attributes, such as a server's operating system or whether a device or host has a particular service enabled.

Fingerprinting capabilities within IPsonar achieve this without disrupting asset operations. Fingerprinting is an important compliment to leak path discovery, prioritizing vulnerability and patch management efforts to vulnerable devices that have exposure to the Internet. IPsonar's Device Fingerprinting:

- Identifies Internet service and proprietary IP applications active on hosts and devices, pinpointing resources for which tested ports are active
- Flags improperly secured wireless access points for remediation, improving security without requiring staff to scan airwaves or deploy antennae-based monitors

- Determines which operating systems network devices are running
- Extracts information from standard packets (i.e., ICMP echo requests and high-port UDP packets); no application layer transactions
- Facilitates consolidation by noting devices that run network-based services, such as printers, network based faxes, and storage appliances

Powerful Visual Analytics

IPsonar offers powerful visual analytics to enable organizations to unleash the value of their networks, driving dramatic improvement in network security and management. IPsonar integrates visualization, interaction, and query capabilities to explore the network data. Users can explore large quantities of information while discovering relationships and patterns leading toward proactive decision making.

For each scan, the report includes maps generated from every IPsonar sensor (i.e., network entry point). In addition, a composite map combines all of the parts of the maps found from the various sensors in a single map.

IPsonar reports thoroughly document the operational state of the network. They are distinct in their explicitness and usability, providing high-level executive summaries along with a technical overview with network drill-down. The reports provide predefined views as a starting point for further analysis.

Continuing Vigilance after the Merger

Even after the M&A process has been completed, it is vital to continue periodically monitoring the network.

Networks are constantly in flux, changing as new technology is implemented, additional M&A activity takes place, or upgrades are handled. Conducting regular scans enables organizations to review the operational state of the network for compliance with security guidelines. IPsonar scans ensure an accurate and unbiased picture of how connectivity flows on the organization’s network and pinpoints unsecured connections and unauthorized connectivity resulting from misconfigured devices.

Using IPsonar, organizations can:
- Compare before and after network maps
- Continue monitoring network changes at regular intervals
- Continue monitoring ongoing risks
- Provide ongoing audit and measurements

Need help getting started?

The Lumeta Network Assessment professional services package is a quick and effective way to "get your arms around your world" – to understand your infrastructure in its totality and establish a network baseline.

- Scope of IP address space in use
- Visibility to the edge of your network
- End-point inventory by volume and type
- A Layer 3 network topology map
- A weighted analysis of network vulnerabilities

www.lumeta.com/mergers

For more information about how Lumeta can help you perform IT due diligence for M&A activities, please email: info@lumeta.com or call +1.732.357.3500.

Lumeta®