Beyond IP Address Management: The Case for Global Ethernet and IP Access Management

An Introduction to IPScan

ViASCOPE USA

Table of Contents

Introduction

Ethernet and IP networks are the defacto standard for a connectivity that is burgeoning in volume and complexity. Ever-growing wired and wireless access across clients, servers, telephony and mobile devices poses a significant management and security challenge to IT departments. While pains have been taken by most IT teams to secure the external perimeter of their networks including deploying firewalls, IDS/IPS, secure VPNs for remote access, and even securing wireless Access Points against war-driving, most IP networks are woefully lacking in controls and auditability over fundamental Ethernet and IP access to the internal network. This lack of visibility, policy enforcement, and auditable documentation on network access creates technical, business and legal liabilities for enterprises. The first section of this white paper explores the current state of Ethernet and IP network access management, and explains the gaps in network address and access management and policy control in today's processes and solutions. The second section introduces a new solution—ViaScope's IPScan, that provides a network-wide, fully automated monitoring, policy enforcement and audit trail capability for enterprise, government, education and service provider IP and Ethernet Media Access Control (MAC) access control. The third section of the white paper explores the benefits and rapid return on investment that dozens of global, Fortune 500-class corporations have experienced in deploying the IPScan solution.

The State of Ethernet/IP Access Management and Control

IP address management, which is the practice of maintaining up-to-date inventories of IP addresses in a network, has been recognized as increasingly important due to a number of factors:

- Webification of applications. An increasing number of applications are utilizing Internet style connectivity standards. In addition, there is increased outsourcing of applications such as customer relationship management (CRM) functions to Internet-based ASPs. These lead to an increased dependence on the network to deliver mission-critical services and applications.
- Voice over IP (VoIP). VoIP phones may potentially double the number of Ethernet/IP devices on a given network. This explosion of networked devices will be increased by Wireless-LAN-compatible mobile devices. VoIP phones in particular not only contribute to the volume of devices, but to the complexity of their connectivity over the network, since VoIP call data flows are peer to peer in nature.
- Internal security threats. According to the CSI/FBI 2004 Survey of Computer Crime and Security, 68% of nearly five hundred surveyed organizations admitted to suffering one or more internal security breaches. A further 32% did not know whether they had suffered an internal vs. external breach. A lack of control over fundamental Ethernet and IP network access opens a dangerous backdoor for internal network abuse.
- The mission-critical nature of IP-based servers and infrastructure components. The lifeblood of an organization's IT infrastructure is proper IP communications. While address conflicts on user's client desktops and laptops cause localized and frustrating outages to individual users or even groups of users, address conflicts affecting critical servers can bring productivity to a standstill, at great cost. It is imperative that continuity of service be preserved, and inadequate address management can directly affect service and application availability.

Most organizations still utilize manual processes and rudimentary tools such as Excel spreadsheets to track IP addresses for management purposes. According to Forrester Research, 25% have developed in-house database solutions, while 20% more have adopted a third party vendor's DHCP management product to help cope with address management.

Yet, today's IP address management approaches and solutions are missing three key ingredients needed to establish sufficient policy-based control over internal network access. These three facets are needed to transcend today's incomplete "address management" processes, to achieve a comprehensive Ethernet and IP *access management* solution.

Lack of Real-Time, Global Coverage:

One of the most important gaps in current processes and solutions for managing Ethernet and IP network access is a lack of timely, global coverage. Manual processes for tracking IP addresses are difficult and time-consuming to maintain, are not updated in real-time, and often miss significant changes in the network. DHCP-based systems, while helpful for allocating IP addresses to users' client devices, don't cover the numerous legitimate, statically addressed servers, switches, routers and other infrastructure devices, non-PC networked devices, as well as hidden and potentially unauthorized statically addressed devices that reside in many IP networks. This partial coverage itself can lead to unintended address conflicts. In addition, the lack of real-time visibility to static IP addresses and their underlying Ethernet MAC addresses means that policy control is inherently limited in scope. Since it is trivial to assign static IP addresses to any IP client device, this is a major hole in internal network access controls and security. Employees or even visitors can easily connect personal laptops and network-attached hard drives, or set up servers without sufficient protections.

Lack of Flexible, Real-Time Enforcement

By definition, most manual processes are strictly documentation tools that cannot enforce any particular IP policy in real-time. DHCP based systems, through their lack of coverage of static devices, cannot enforce policy in a global fashion.

The one solution that has been applied to attempt to enforce address controls is inflexible—locking particular Ethernet MAC addresses to specific Ethernet switch ports. However, the realities of WLAN access, and roving and transient nature of today's network users including traveling employees, partners, customers and contractors, make this inflexible method insufficient to enforce network access policy. With significant portions of IP networks relegated to manual address management, the reality is that the vast majority of organizations cannot effectively enforce any Ethernet and IP access control policy.

Lack of Complete Historical Documentation and Audit Trail

Due to the lack of coverage of all networked devices, today's processes and solutions for address management don't provide the historical audit trail needed to properly troubleshoot problems, and to establish documentation for regulatory auditing purposes.

For network administrators trying to deal with a constant and often overwhelming load of trouble tickets, the invisibility of networked devices can cause hours of wasted time and productivity trying to track down devices that may be causing disruptive address conflicts or may be a security threat. Without a full set of real-time and accurate host-level documentation, finding an offending host can be trying to find a needle in a haystack.

Trying to manually keep accurate records of hundreds or thousands of Ethernet/IP hosts is inherently inefficient, wasting hours of expensive IT personnel time, and furthermore tends to fall into the category of administrative tasks that are always neglected due to the routines of daily fire-fighting. This lack of documentation can ultimately lead to costly effects for the organization, when downtime or security lapses are increased because troubleshooting is slowed by poor network documentation.

If a lack of comprehensive and global networked device documentation prevents IT staff from effectively troubleshooting threats to the network's integrity and security, it is a clear signal that there are insufficient controls to prove compliance to regulatory requirements for data security. This is particularly important given the highly publicized breaches of consumer privacy and shareholder rights that have spurned greater regulation over data security. Whether Sarbanes-Oxley (SOX), HIPAA, Gramm-Leach Blilely, non-compliance with regulations concerning sensitive data can be very costly. Without a full, network-wide and comprehensive system to ensure policy compliance and a historically accurate, network-wide audit trail of network access policy controls and user actions, it is difficult to prove that proper controls are in place, leaving organizations open to potential penalties and even criminal liabilities.

Introducing IPScan: Global Ethernet and IP Access Control

A new, more comprehensive approach to Ethernet and IP access management is now available to IT departments, that provides global, network-wide policy control and monitoring of all Ethernet/IP devices. ViaScope's IPScan is utilized today by dozens of global, Fortune-500 class enterprises, service providers, government and military agencies and educational institutions, to establish effective policy-based control over their whole Ethernet and IP infrastructure, including access control and address management.

IPScan enables IT departments to retain central command of their networks – by controlling fundamental access to the internal network's edge at the Ethernet MAC and IP layers. This network edge is the place where users and applications connect, where traffic enters and exits the network. The network edge is where security policies can be enforced most effectively, where the IP devices gain access to the network, whether with a static or dynamic IP address.

An appliance-based solution, IPScan offers an easy to deploy solution that requires no intrusive client software, and that provides the following building blocks for effective IP/Ethernet Access Control:

- Global Scope: Real-time auto-detection and monitoring of all IP/MAC devices on the network, including both statically and dynamically addressed devices, whether wireless or wireline-connected.

- Flexible, Real-Time Enforcement: Policy-based, automatic admission or blocking of any IP/MAC device, without needing to manually assign addresses to physical devices such as Ethernet switch ports

- Transparent operation from within the network, requiring no client software and retaining full network flexibility

- Powerful, centralized policy definition, monitoring and alerting

- Full historical documentation and audit-trail of all IP/MAC device connectivity

IPScan provides complete Ethernet and IP access security that includes pre-set policies that apply to any combination of IP and MAC addresses, and even hostnames. IPScan's central information structure provides control of individual user access as well as a clear audit trail so a company can track and monitor network activity.

How IPScan Works

The IPScan solution consists of distributed IPScan probe appliances that perform the real-time auto-detection, monitoring, policy enforcement and alerting. A centralized IPScan console server and client application provide the administrator with policy definition, global monitoring information, real-time policy enforcement controls, and the historical audit trail.

An IPScan Probe appliance interfaces with Ethernet switches and passively monitors all Ethernet and IP devices that attempt to access the network. The probe compares the source MAC and IP address information of new devices against all the relevant registered/authorized MAC addresses downloaded from the IPScan servers' database. If the MAC or IP address has not been pre-registered as an authorized device, the IPScan Probe can automatically block the device from communicating with other hosts on the network, and send an alert to the central console. This enforcement works whether the device is dynamically or statically assigned an IP address.

IPScan allows an IT manager to centrally control access to an entire network, across multiple sites from a single console. IPScan does the same job within a wireless networked environment – preventing unauthorized WIFI 802.11 access. It also has a Time Control feature that allows administrators to define the time of day and day of week that a guest can access your network, as well as a maximum inactivity period, so that devices that haven't connected to the network within a set period of time revert to an unauthorized state.

The IPScan Console gives the IT manager real-time access control and policy administration power. Since every IP device is monitored by the IPScan Probe, any device or group of devices can be blocked or 'kicked off the network' instantly by selecting the IP, MAC address or node name, and choosing the 'block' option from within the IPScan console.

The IPScan Console allows the IT manager to create groups and categorize IP addresses into physical and logical segments, such as servers, printers, network devices, or, accounting, sales, and operations. Access control or complete denial of access can be applied to a single IP/MAC or a range of address. This allows the administrator to easily apply customized policies to different users or classes of users.

The IPScan solution also prevents all duplicate IP address and related conflicts on the network by documenting bindings between every IP and MAC address within each network segment. This practically eliminates the downtime that can occur when a rogue device conflicts with a critical infrastructure component such as a server or router.

IPScan's Benefits and Rapid Return on Investment

IPScan provides a number of benefits to organizations looking to enforce greater controls over Ethernet and IP network access and addressing.

Increased Security

IPScan provides much greater internal network security by ensuring that every device that connects to the network has an authorized Ethernet and IP address, and even hostname. When used in conjunction with other sound network access controls, IPScan greatly mitigates against the risk of costly internal security breaches.

Reduced Downtime from Address Conflicts

Forrester Research reports that 15% of overall downtime in enterprises is due to network issues, with a majority of that network-based downtime attributed to addressing issues. By eliminating address conflicts, IT departments can prevent frustrating user downtime and mission-critical server downtime.

Seamless Integration with Existing IP Networks

A fundamental principle of IP network deployment is to locate intelligence, authentication and security at the edge of the network, while allowing the core of the network to perform simpler routing and switching tasks. IPScan's enforcement model aligns with this architectural principle, since it controls access at the network's edge. This architectural simplicity and integrity keeps the solution simple, allowing it to co-exist seamlessly with other network components.

Enhanced Compliance Posture

IPScan gives corporations the ability to construct an intelligent access control solution that administrates central policies over the entire WAN, and the continuous historical documentation to prove that it has clearly defined and enforceable network access policies to any regulatory or auditing body.

Ease of Deployment and Low Overhead Operation

Unlike many security solutions that require extensive client software deployment, IPScan allows IT departments to gain significantly greater control over their networks without the added overhead of installing and maintaining client software. This means that users don't require additional training, nor will administrators be saddled with yet another set of tasks. In addition, IPScan allows IT departments to unify access control processes between wired and wireless devices, further reducing overhead.

Streamlined IT Operations

IPScan automates 80% of the job of IP address management, a time-consuming yet necessary task that consumes network administration productivity. By deploying IPScan, IT can reclaim skilled network managers' productivity to work on strategic IT initiatives. In addition, IPScan's automation, real-time enforcement and global host-level visibility and documentation enable IT to respond to customer and business requirements with greater and speed and accuracy.

These benefits lead to a rapid return on investment. For more information on the business case for IPScan, please read the ViaScope white paper entitled, The Case for Secure Ethernet and IP Access.

Conclusion

IPScan provides a comprehensive solution for global, auditable network access and address management of Ethernet and IP devices. IPScan enables IT departments to significantly reduce the risk of internal security breaches, eliminate address conflicts, enhance regulatory compliance readiness and streamline operations.

To learn more about IPScan, contact VIASCOPE USA at 1-877-IP-SCANN, email us at sales@viascopeus.com. Or visit our website at: http://www.viascope.com.