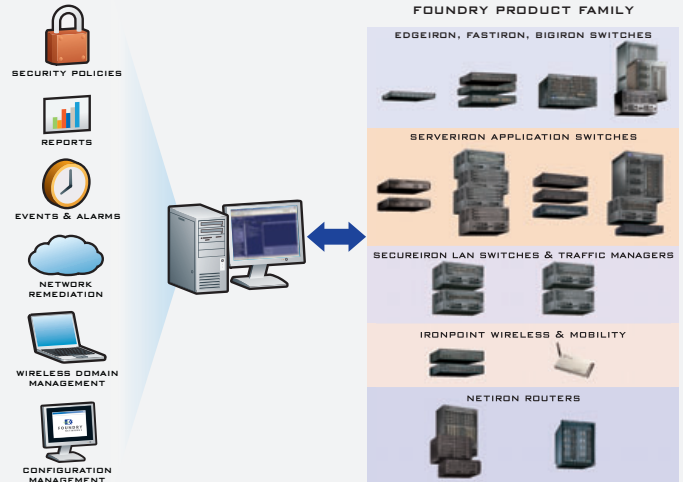


IronView Network Manager



FOUNDRY
NETWORKS

IronView™
Network
Manager



**RELIABLE, SCALABLE, AND
SECURE NETWORK MANAGEMENT**

KEY HIGHLIGHTS

- ▶ Fault, configuration, accounting, performance, and security management (FCAP) for Foundry's complete product line
- ▶ Flexible, scalable architecture that can support 1000s of Foundry devices in large organizations with highly distributed environments
- ▶ Dashboard and thumbnail views of wired and wireless devices, current status, event and alarm summary, and network visibility for troubleshooting and analysis
- ▶ IPv6 support on INM and Foundry devices
- ▶ Powerful search capabilities to enhance productivity
- ▶ Comprehensive security management capabilities, including IronShield 360 Closed Loop Security
- ▶ Network topology discovery, with L2, VLAN, IP subnet, STP/RSTP, MRP Ring views and multiple layout and sizing tools
- ▶ Interface and integration with HP OpenView
- ▶ Enhanced SNMP collection and display
- ▶ Rapidly deploys group network and policy changes
- ▶ Supports all Foundry product families
- ▶ Configurable and flexible user-based bandwidth, access control list, and rate limiting policy support
- ▶ Central management of all wireless and mobility products
- ▶ Standards-based, highly secure network management system built on Java, SNMP, and sFlow (RFC 3176)
- ▶ Supported on Windows, Linux, and Solaris

Foundry's IronView Network Manager

Foundry IronView™ Network Manager (INM) provides network administrators with comprehensive tools for configuring, managing, monitoring, and securing Foundry's award-winning line of wired and wireless network equipment. INM is an intelligent network management solution that reduces the complexity of changing, monitoring, and managing network-wide features such as Access Control Lists (ACL), rate limiting policies, VLANs, software and configuration updates, and network alarms and events.

With INM's intuitive and easy-to-use Web-based tools, networks are less prone to outages due to incorrect configurations or invalid software upgrades. Built on a Java-based platform, Foundry INM lets network operators seamlessly control software and configuration updates for any Foundry product from anywhere in the network, enabling more effective management of medium and large networks.

Using INM, network managers can automatically discover Foundry network equipment and immediately acquire, view, and archive configurations for each device. Group policies can

be easily configured and deployed for Foundry's wired and wireless products, including security requirements, rate limiting, and event management policies.

INM takes advantage of the Foundry high-speed, secure architecture, with integrated sFlow technology, described in RFC 3176, to deliver hardware-based and real-time network monitoring and accounting capabilities. These features ensure wire speed switching and routing performance with "always-on" fault and performance management, capacity planning, intrusion detection, security policing, and precise network traffic accounting.

INM Key Features and Benefits

INM 3.0 application features simplifying network management and enhancing productivity when managing Foundry products. The following key application managers and features are included in INM 3.0:

- ▶ INM Dashboard
- ▶ Administration Manager
- ▶ Topology Manager
- ▶ Device Configuration Manager
- ▶ MAC Filter Manager
- ▶ Access Control List Manager

INM 3.0 New Features and Enhancements

New and enhanced features in INM 3.0 include:

FEATURE/ENHANCEMENT	DESCRIPTION
Enhanced Dashboard Reports	Drill down capability of dashboard elements
Enhanced Topology Manager with support for MRP and STP/RSTP Topology View	Coordination of Topology Views, right-click support to launch items from Topology View
INM trap forwarding to other NMS	Ability to forward SNMP traps to other NMS such as HPOV or to INM itself
Enhanced Event Processing/Event Action Configuration	Ability to apply threshold settings of INM generated traps to generate event actions
Enhanced Closed Loop Security	Parse SNORT rules file and create a set of INM-specific SNORT messages
Enhanced search capability including Regular Expression Based Search	Search in NOM, Topology Maps and Change Manager. Search by text, regular expression, image version, build level
IPv6 support including support for IPv4 and IPv6 simultaneously	IPv6 support including IPv6 management access and IPv6 remote management. Also includes IPv6 sFlow support
Automated database backup	Users can configure INM to back up the INM database
LLDP Discovery support	In addition to FDP (Foundry Discovery Protocol), LLDP (Link Layer Discovery Protocol) can be used to discover neighbor nodes
Enhanced sFlow Report	sFlow reports now contains Reverse DNS Lookup
Enhanced wireless services including ADC and AP Session Report scalability	New ADC version 3.0 support AP current session report now supports higher Current scalability numbers (1000+ APs)
Pre/Post Snapshot	User defined CLI command to capture pre/post snapshots of device
User restriction to specific ServerIron Virtual IPs	Different AoR (Areas of Responsibility) support for ServerIron VIP and real server IP address
Device Resync password updates	Device passwords that are changed off-line are now updated when INM initiates a re-sync
Single Subnet Discovery Support	Ability to discover devices in a single subnet without re-discovering all of the previously discovered devices
INM Server Restart from Client Browser	INM users can now restart the INM server from their remote browser
ICMP Ping Support	ICMP ping support in addition to TCP ping

- ▶ Rate Limiting Manager
- ▶ Change Manager
- ▶ ServerIron Traffic Manager
- ▶ SecureIron Denial-of-Service Manager
- ▶ Event Manager
- ▶ Report Manager
- ▶ RF Monitoring Manager
- ▶ Service Director
- ▶ IronPoint Wireless Family of Management Solutions
- ▶ IronShield 360 Security—Closed Loop Intrusion Detection and Prevention

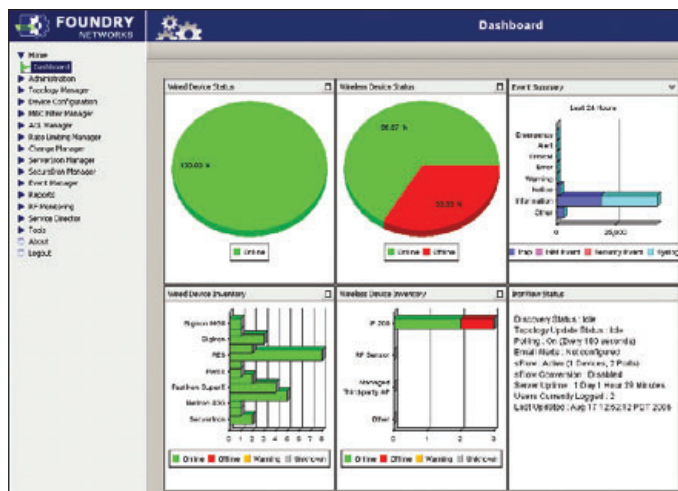
INM's application managers are Web-based, allowing network managers to access network elements from anywhere using any well-known browser, while keeping access independent of client and operating system. With INM, network operations can be performed from anywhere, and at any time, especially when network changes may be critical.

INM also provides several ways to secure access to Foundry devices. Network managers can select from a number of network console capabilities, such as SSH, Telnet, SCP, or TFTP to access a device and get status or execute commands through a CLI. They can also obtain access through a Web management interface using either HTTP or secured HTTP (HTTPS).

INM Dashboard

The INM dashboard shows information about Foundry devices, including asset views, status and alarms, and INM status. Thumbnail views can be saved and easily printed for historical purposes.

Views include a wired and wireless device status pie chart and an inventory bar graph showing the number and family type of each Foundry device discovered. An event summary bar chart shows the number and type of events for each severity defined by INM, and event types include traps, internal INM events, security events (for Snort or partner security events), and syslog events. This bar graph can also show the event summary for the last 24 hours, 7 days, or 30 days. When clicked, each element in the INM dashboard provides detailed information. For example, if the user clicks an event type in the event summary pane, an events report for is displayed.



The INM status window in the dashboard shows internal INM processes, including:

- ▶ Discovery status
- ▶ Topology status
- ▶ Polling interval
- ▶ Email alert status
- ▶ sFlow collector and PCAP conversion status
- ▶ Server uptime
- ▶ Number of active management users
- ▶ Last update timestamp

Administration Manager

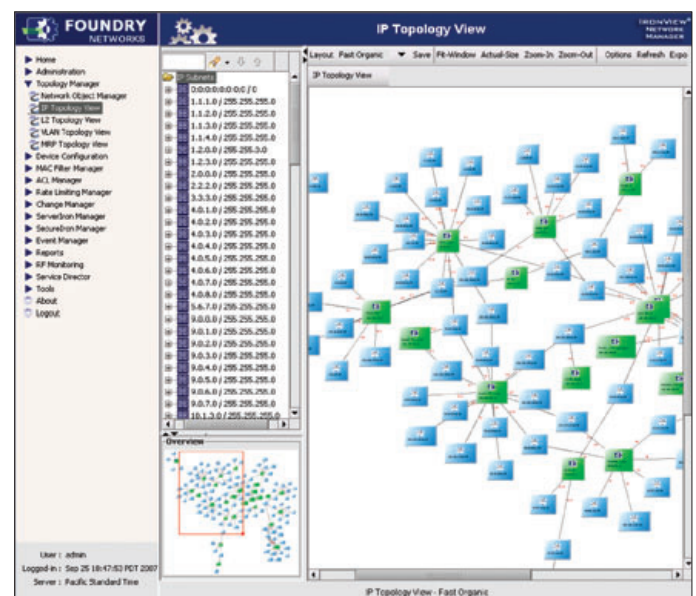
INM Administration Manager contains key sub-managers that control INM access, global settings, and network discovery.

The User and Role Manager assign access, security levels and configuration authority to individuals and groups, securely separating common tasks across multiple management entities. User actions are recorded to display configurations deployed within a Foundry device or group of devices, allowing network managers to view the configurations used during deployment and troubleshoot any network problems that may result. Secure authentication methods such as TACACS+ or AAA simplify the security system for INM users, and for users accessing any Foundry products.

The Discovery Manager monitors the discovery process for periodic network topology updates, and has a Topology Configuration sub-manager that allows the export of topology data to HP OpenView Network Node Manager (NNM).

Topology Manager

The INM Topology Manager integrated topology discovery and network map capability allows layer 2, VLAN, IP subnet, STP/RSTP and MRP Ring views of Foundry devices. The powerful search tool quickly locates devices based on text (IP or name of device), regular expression, image version, or build level. Individual nodes and groups of nodes can be selected for fixed placement on the map when zooming. Nodes are shown with detailed information, including name, IP address, trunk groups, and interface names. Detailed reports can be quickly configured and generated for all Foundry devices in the map.



The Network Object Manager sub-function provides a view of each Foundry network element, together with key administrative values such as passwords, community strings, and other authentication attributes.

Network managers can create groups based on devices or ports using Device and Port Groups within Topology Manager. They can also filter the device tree to display only devices of a specific type or current operating status to quickly deploy configuration changes, load common configurations, and perform common monitoring functions.

Device Configuration Manager

The INM Device Configuration Manager provides tools for configuring, managing, and deploying wireless and wired devices through multiple sub-managers:

- ▶ Configuration Wizard—allows configuration payloads to be defined and then rapidly deployed to targeted wireless and wired devices.
- ▶ VLAN Manager—enables network managers to discover already configured VLANs and perform addition, moves, and changes to any VLANs within their network.
- ▶ Realm Manager—allows wireless realms to be defined, configured, and managed in the Foundry IronPoint 200/250 wireless access points.
- ▶ Automatic Discovery and Configuration (ADC) Manager—allows the dynamic discovery and configuration of Foundry wireless access points, and provides central AP management.
- ▶ Wireless Mobility Manager—allows Foundry wireless LAN switches to be grouped into domains for layer 3 mobility support.
- ▶ CLI Configuration Manager—allows CLI commands to be executed against specific devices or groups of Foundry devices. This powerful tool provides a text-based interface through which network administrators enter CLI commands to create device configurations and reports.

Access Control List Manager

Access Control List (ACL) Manager allows rapid configuration and deployment of ACLs in Foundry's wired and wireless switches, routers, and access points. ACLs allow devices to permit or deny packets based on their source and destination MAC or IP addresses, IP protocol, or TCP/UDP protocol values. Using ACL Manager, network managers can import ACLs from a Foundry device or a group of Foundry devices, move existing ACLs within the ACL Manager, and redeploy existing ACLs in other Foundry devices.

The ACL Manager has three sub-applications:

- ▶ Service Manager—allows network managers to use pre-defined and well-known service ACLs, providing flexible and simple mechanisms to create, add, and deploy ACLs using “named” services. In addition, the ACL Service Manager can add new UDP or TCP ports to the named service functions.
- ▶ Network Manager—allows users to add and group IP subnets or IP addresses.
- ▶ Layer 2 Manager—allows Layer 2 ACLs to be easily defined and deployed across individual or groups of Foundry devices.

MAC Filter Manager

The INM MAC Filter Manager supports the configuration and deployment of MAC filters on Foundry wired and wireless devices that support them. MAC filtering capabilities allow permit and deny functions to be configured for source and destination MAC and Ethernet type. Both wired and wireless MAC filters can be imported into INM from Foundry devices.

Event Manager

The INM Event Manager helps network managers to troubleshoot network-related problems. The Event Manager can receive SNMP traps, Syslog events, Snort, and security partner event messages for reporting, analysis, monitoring, and remediation, and can alert network managers proactively to any events INM is configured to analyze. The Trap Forwarding feature allows INM to filter SNMP traps, and pass them to third party applications capable of managing events from different equipment vendors. Event Manager can use Foundry's CLI configuration manager to support full closed-loop network remediation. Under the IronShield 360 umbrella, INM Event Manager can accept events from open source software, such as Snort, and third-party security products, and act on these events based on user-defined security policies.

Service Director

The INM Service Director provides management tools for sFlow and SNMP-based data collection, reporting, accounting, and presentation. The Service Director custom report generator allows network managers to define any set of reports based on the data collected from sFlow.

Report Manager

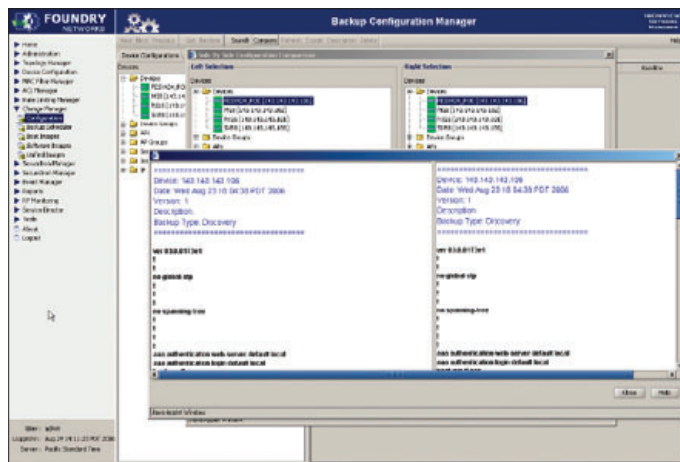
The INM Report Manager provides a rich set of pre-defined asset reports with details on dynamically or statically discovered wired and wireless devices, as well as key attributes, such as name, IP address, version information, product type, last scan day/time, and status.

The library of pre-defined asset reports include:

- ▶ Wired and Wireless Devices
- ▶ Modules and VLANs
- ▶ IP Subnets, IP, and MAC Addresses
- ▶ AP Current Session, Session History, Throughout, Usage

Change Manager

INM Change Manager helps network administrators view, retrieve, and restore configuration files. During the discovery process, copies of the device configurations are imported into INM. Change Manager can be scheduled to automatically backup configurations, or backup can be done manually. The pre/post snapshot feature allows device configuration, VLAN and MAC filter payloads to issue device monitoring commands before, after, or before and after a configuration change is deployed. Configurations can be compared and contrasted to quickly spot problems during configuration deployments, and can be used to roll back to a previous configuration if needed.



Change Manager also allows software, diagnostic, and boot images to be manually or automatically imported into INM. Multiple versions of software can be stored in INM, and may be deployed to devices directly by the network manager.

ServerIron Traffic Manager

The INM ServerIron Manager provides both Virtual IP Address (VIP) server management capabilities and Global Server Load Balancing (GSLB) management of the Foundry ServerIron Application Traffic Manager products.

VIP Server Manager functions include:

- ▶ Display of VIPs configured on a ServerIron
- ▶ Display of virtual server and real server port bindings configured on a ServerIron
- ▶ Display of real server and virtual server port status
- ▶ Enabling and disabling real or virtual server ports

INM GSLB Manager supports configuration and monitoring of GSLB capabilities (such as policy, site, zone, and controller management, monitoring, and deployment) in the ServerIron product family. Key statistics and events for GSLB can be monitored in real-time, including:

- ▶ GSLB resource monitoring
- ▶ Global statistics monitoring
- ▶ DNS detail monitoring
- ▶ Site, traffic, policy, and host status

SecureIron Denial-of-Service Manager

INM SecureIron DoS Manager provides centralized management services for Foundry's SecureIron family of security products. DoS Manager provides tools for the creation and display of generic and pre-defined SecureIron signature rules, as well as the definition and display of filters (collection of rules and actions), including the ability to define multiple actions (log, drop). Using the controller, INM's DoS Manager can rapidly deploy filters on groups of SecureIron devices and across multiple interfaces.

INM DoS Manager allows SecureIron Traffic Managers and SecureIron LAN Switches to be rapidly and easily configured, deployed, monitored, and managed, which significantly lowers the total cost of ownership of an organization's security devices. All of the wired, wireless, security, and traffic management solutions can be managed and monitored from a single console.

IronPoint Wireless Family of Management Solutions

INM includes central management support for the entire family of Foundry wireless products and solutions, including the IronPoint IP200 wireless access point, IronPoint switches, and the IronPoint Mobility Controller series. With INM, Foundry access points can be automatically discovered and configured through the Automatic Discovery and Configuration (ADC) Manager.

INM's RF monitoring capabilities allow IronPoint RF sensors to identify and prevent access to rogue access points and ad-hoc client networks. INM collects and analyzes data from Foundry RF Sensors to generate rogue AP and ad hoc alerts and reports.

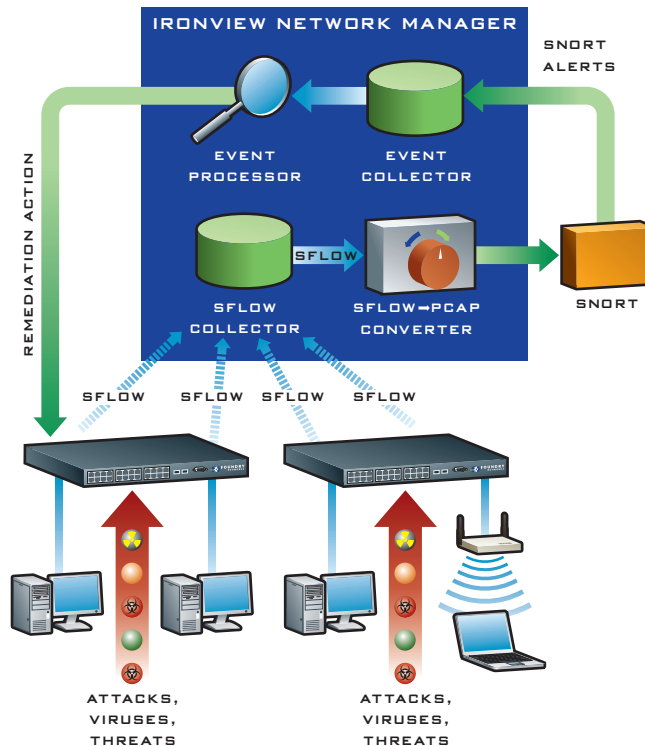
For significantly enhanced scalability, the FastIron Edge Wireless LAN (FES-WLAN) switch can be used to offload the management of IP200 wireless access points. INM can then manage the FES-WLAN switches rather than manage each AP separately.

IronShield 360 Security and Intrusion Detection

INM provides many options for gathering data from Foundry network devices, including support for both SNMP and sFlow collection. SNMP data collection provides a high level view of what is happening in the network, while sFlow collection provides the unique view of network traffic in real time. INM's sFlow collection capability is ideal for generating traffic reports and gaining visibility into network activity, even at the edge, where placing sensors is costly and difficult. sFlow collection capability can be integrated with open source IDS software, such as Snort, to provide the industry's first full closed-loop intrusion detection, prevention, and remediation capability.

With IronShield 360, the sFlow collection modules within INM can convert sFlow to the open source PCAP format. The PCAP data can then be piped directly into Snort and other open source IDS software to spot accidental or malicious network activity and send alerts to INM through the IDS Event Manager. INM can then take direct remedial action on this network activity, through its unique security policy manager. This powerful capability turns INM into a full intrusion detection and prevention solution. Because sFlow is available on all Foundry switches and routers, INM cost-effectively detects and prevents intrusions throughout the network, even at the edge.

INM processes events and takes remedial action for a number of Foundry's anomaly detection partners. By extending our event processor to handle events from our IronShield 360 security partners, INM provides the industry's first closed-loop security and management solution for both signature and anomaly detection solutions.



System Requirements

The INM software and documentation are shipped on a CD-ROM. In addition to a CD-ROM drive, your system must meet the requirements shown in Table 1 to successfully install INM.

Table 1. INM Server Requirements

	WINDOWS	SOLARIS	LINUX
Minimum OS version	2003 Server (SP2) XP Professional Edition (SP2)	9 and 10	Red Hat Enterprise Linux WS Release 4
Minimum CPU and Speed	<ul style="list-style-type: none"> • 1–200 devices: 2.0 GHz Pentium 4 with 2 GB of RAM (minimum), 3.0 GHz Pentium 4, 3 GB of RAM (recommended) • 200–1000 devices: 2.0 GHz Dual Core CPU with 3 GB of RAM (minimum), Multi Core Xeon Processor 3000 sequence or above (or similar AMD processor) with 4 GB of RAM (recommended) • 1000+ devices: Dual (or more) Xeon 5000 sequence or above (or similar AMD processor) with 4+ GB of RAM (recommended) 	<ul style="list-style-type: none"> • 1–200 devices: Sun UltraSPARC T1 (or similar UltraSPARC processor) with 2 GB of RAM (recommended) • 200–1000 devices: Sun UltraSPARC T2 (or similar UltraSPARC processor) with 4 GB of RAM (recommended) • 1000+ devices: Sun UltraSPARC T2+ (or similar UltraSPARC processor) with 4+GB of RAM (recommended) 	<ul style="list-style-type: none"> • 1–200 devices: 2.0 GHz Pentium 4 with 2 GB of RAM (minimum), 3.0 GHz Pentium 4, 3 GB of RAM (recommended) • 200–1000 devices: 2.0 GHz Dual Core CPU with 3 GB of RAM (minimum), Multi Core Xeon Processor 3000 sequence or above (or similar AMD processor) with 4 GB of RAM (recommended) • 1000+ devices: Dual (or more) Xeon 5000 sequence or above (or similar AMD processor) with 4+ GB of RAM (recommended)
Minimum RAM Requirement	2 GB	2 GB	2 GB
Maximum RAM Requirement	120 GB	120 GB	120 GB

Table 2. INM 3.0a Client Requirements (required to access any Web-based INM application)

	WINDOWS 2003, 2000, OR XP PROFESSIONAL EDITION	SOLARIS 8, 9, AND 10	RED HAT ENTERPRISE LINUX WS RELEASE 3 AND 4
Internet Explorer Browser	IE 6.0 and above	Not Supported	Not Supported
Mozilla Firefox	Firefox 2.0	Firefox 2.0	Firefox 2.0
Java Plug-In	JRE-1.5.0_12	JRE-1.5.0_12	JRE-1.5.0_12

Table 3. INM 3.0b Client Requirements (required to access any Web-based INM application)

	WINDOWS 2003, 2000, OR XP PROFESSIONAL EDITION	SOLARIS 8, 9, AND 10	RED HAT ENTERPRISE LINUX WS RELEASE 3 AND 4
Internet Explorer Browser	IE 6.0 and above	Not Supported	Not Supported
Mozilla Firefox	Firefox 2.0	Firefox 2.0	Firefox 2.0
Java Plug-In	JRE-1.6.0_05	JRE-1.5.0_15	JRE-1.5.0_15

Specifications subject to change without notice.



Foundry Networks, Inc.
Corporate Headquarters
4980 Great America Parkway
Santa Clara, CA 95054

U.S. and Canada Toll-free:
1-888-TURBOLAN (887-2652)
Direct telephone: +1 408.207.1700
Fax: +1 408.207.1709

Email: info@foundrynet.com
www.foundrynet.com

Foundry Networks, Inc. (NASDAQ: FDRY) is a leading provider of high-performance enterprise and service provider switching, routing, security and Web traffic management solutions, including Layer 2/3 LAN switches, Layer 3 Backbone switches, Layer 4-7 application switches, wireless LAN and access points, metro and core routers. Foundry's customers include the world's premier ISPs, metro service providers, and enterprises, including e-commerce sites, universities, entertainment, health and wellness, government, financial and manufacturing companies. For more information about the company and its products, call 1.888.TURBOLAN or visit www.foundrynet.com.

The foregoing may contain "forward-looking statements" which are based on management's current information and beliefs as well as on a number of assumptions concerning future events made by management. These forward-looking statements include, without limitation, statements by executives or spokespeople regarding Foundry's positioning and potential plans. The forward-looking statements are only predictions and are subject to a number of risks and uncertainties, which could cause actual results to differ materially. Foundry assumes no obligation to update the forward-looking statements contained in this document. Furthermore, no statements made by Foundry Networks, Inc. ("Foundry"), or information contained herein, may be deemed to constitute either an amendment of an existing agreement or an implied new commitment, promise or legal obligation by Foundry to develop or deliver any specific product, feature or functionality.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>). This product includes software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (glh@cryptsoft.com).

© 2008 Foundry Networks, Inc. All Rights Reserved. Foundry, Foundry Networks, BigIron, Netron, IronShield, IronView, IronWare, JetCore, JetScope, MetroLink, Terathon, TrafficWorks, Power of Performance and the 'Iron' family of marks are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries. sFlow is a registered trademark of InMon Corporation. All others are trademarks of their respective owners.
FDRY_DS-013_IP_2008_09_Rev06