Eagle-Eyes Network Monitoring

Hinx Limited - Network Consultants

Network downtime costs your company money. Any network problem requires an experienced eye to quickly find the root cause of any problem, and that experience can be hard to find. The quick resolution of any network problem saves modern businesses millions of pounds every year.

Eagle-Eyes is an appliance from Hinx Limited, a specialist provider of technical networking services built on many years of experience that aims to speed up problem resolution – or even predict and prevent problems from occurring.

Eagle-Eyes uses a hardened Linux server as its' base, making the overall system immune to many of the threats that network servers face. This server polls networking equipment regularly to gather a wealth of status information from the network. There are two major differences between *Eagle-Eyes* and a standard network management platform:

- Knowledge of important network links (i.e. between switches or routers)
- Alerting (email and/or text-message based) of only important events – or of a critical combination of minor events that signal unusual failure.
- Trending and auto-baselining – determining what is "normal" on a network and providing an indication of when the traffic levels are outside of those "normal" parameters.

Eagle-Eyes offer the client several additional benefits: a web browser interface that allows examination of all data held about the network's operations and health.

Having a base-line of information also allows for easy determination of "peaks" to see where unusual activity is occurring and to determine what should constitute an alert and what should not.

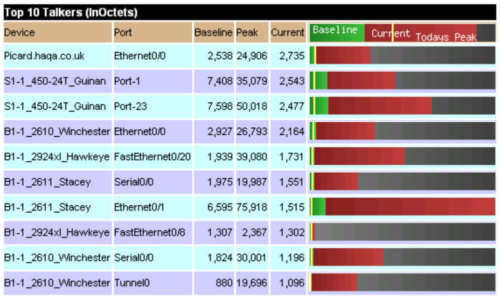
Hinx have used their many years collective expertise in troubleshooting networks to build a rule-base into the intelligent system to all but eliminate "false positives" and to use this valuable monitoring tool to collate information about the network elements (switches and routers).

Eagle-Eyes does not monitor the health of servers or printers (although it can be configured to do so), it is intended as a best-in-class network monitoring tool.

Passive Monitoring Server

The *Eagle-Eyes* service uses a passive monitoring server, which is located in the client's network. This server gathers SNMP information about the network, collecting basic information on CPU usage, key network link usage and other metrics from the networking hardware.

These simple statistics are collated in a database on the server, and presented on graphs showing the statistics over time with various timescales. The server collects statistics every 5 minutes, by examining many SNMP variables in the networking equipment.



Top 10 Talkers (InOctets)

Device	Port	Baseline	Peak	Current	Baseline Current Todays Peak
Picard.haqa.co.uk	Ethernet0/0	2,538	24,906	2,735	
S1-1_450-24T_Guinan	Port-1	7,408	35,079	2,543	
S1-1_450-24T_Guinan	Port-23	7,598	50,018	2,477	
B1-1_2610_Winchester	Ethernet0/0	2,927	26,793	2,164	
B1-1_2924xl_Hawkeye	FastEthernet0/20	1,939	39,080	1,731	
B1-1_2611_Stacey	Serial0/0	1,975	19,987	1,551	
B1-1_2611_Stacey	Ethernet0/1	6,595	75,918	1,515	
B1-1_2924xl_Hawkeye	FastEthernet0/8	1,307	2,367	1,302	
B1-1_2610_Winchester	Serial0/0	1,824	30,001	1,196	
B1-1_2610_Winchester	Tunnel0	880	19,696	1,096	

A "Top talkers" database is maintained automatically, collating information from 9 important metrics from every router or switch port in the network, holding baseline trend information for immediate recall – so you can instantly see any ports that are exhibiting atypical behaviour.

All collated information can be viewed using a simple web browser, available from anywhere on the internal network. All pages can be password-protected so that only IT staff may view privileged information.

Eagle-Eyes Network Monitoring

Hinx Limited - Network Consultants

Where the network is being maintained by both internal and external resources, a change control system must be followed to ensure that all parties involved are aware of changes. Outages may have to be planned, or emergency action taken. In either case, change control procedures must be followed to ensure that the network is in a known state.

Even the smallest change to the network can have critical impact, and having a clear list of changes is fundamental in being able to track such changes, including the individual responsible for those changes.

The overall “health” of the network is an important metric. The time to bring in an expert eye is when the first symptoms are seen. Having EagleEyes brings these alerts into sharp focus, usually well before trouble is caused.

Alerts

The *Eagle-Eyes* system does much more than just monitor the network. The system learns the behaviour and configuration of the network over a period of time and can then send out email or even SMS alerts when particular thresholds are exceeded.

This particular feature provides early warning of network problems. Any spike in CPU utilisation (a common indicator of a network protocol problem) will be instantly recognized by the alerting software and a resultant alert will bring Hinx expertise into focus upon the problem within minutes[1].

These alerts aim to provide IT staff with information, which can be acted on quickly. Often these will indicate the areas for further investigation, and Hinx expert consultants can often quickly diagnose these faults.

Hardened Server platform

The passive monitoring server runs Linux, hence is not prevalent to Microsoft-biased network worm attacks. This server runs a suite of open source software programs known collectively as “EagleEyes”. EagleEyes is a passive software system that will contain configuration information about the network, including all network switches, routers and the firewall(s).

[1] Depends on service contract and may require *Safe Hands* subscription

Vendors covered

CISCO SYSTEMS

At present *Eagle-Eyes* is focused around the industry-leader, Cisco Systems, although other vendors will be incorporated.

Other vendors considered for future incorporation include:

ProCurve Networking HP Innovation

FOUNDRY NETWORKS

extreme networks

Document Number BR-1706

Hinx Limited

20 Lovell Close
South Wonston
Winchester
SO21 3EN

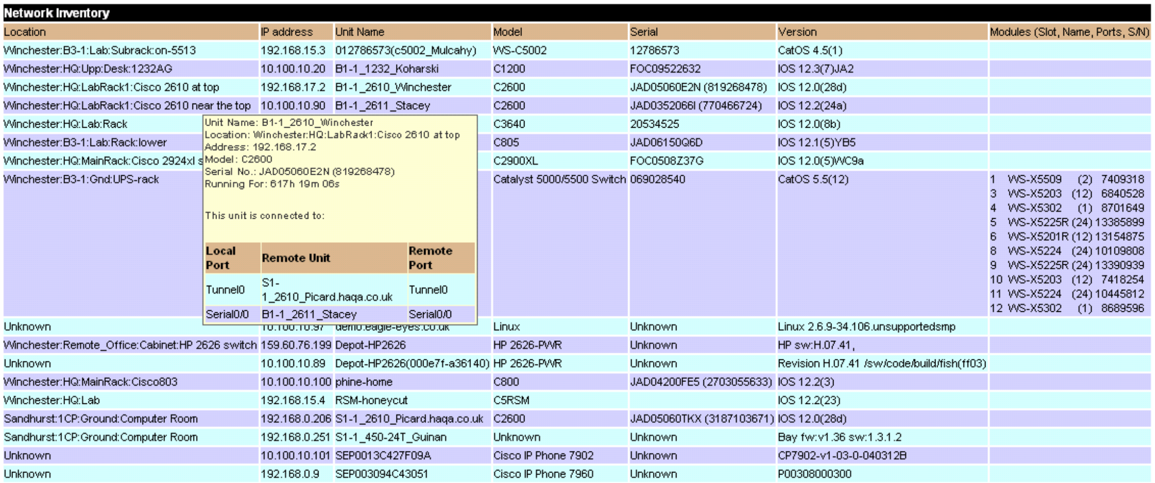
Tel: 01962 886 174 Fax: 01962 885 705

http://www.hinx.com mailto:sales@hinx.com

Additional Modules

EagleEyes doesn't just keep track of your network, it provides an invaluable "what happened recently" archive for experts to view – which can dramatically reduce the amount of time taken to pinpoint and fix networking problems. The following modules are planned for release during 2006:

Network Inventory – keeping track of the serial numbers and versions of all your networking infrastructure equipment, including modular switches and routers.



Network Inventory

Location	IP address	Unit Name	Model	Serial	Version	Modules (Slot, Name, Ports, S/N)
Winchester:B3-1:Lab:Subrack:on-5513	192.168.15.3	012786573(c5002_Mulcahy)	WS-C5002	12786573	CatOS 4.5(1)	
Winchester:HQ:Upp:Desk:1232AG	10.100.10.20	B1-1_1232_Koharski	C1200	FOC09522632	IOS 12.3(7)JA2	
Winchester:HQ:LabRack1:Cisco 2610 at top	192.168.17.2	B1-1_2610_Winchester	C2600	JAD05060E2N (819268478)	IOS 12.0(28d)	
Winchester:HQ:LabRack1:Cisco 2610 near the top	10.100.10.90	B1-1_2611_Stacey	C2600	JAD0352066I (770466724)	IOS 12.2(24a)	
Winchester:HQ:Lab:Rack			C3640	20534525	IOS 12.0(8b)	
Winchester:B3-1:Lab:Rack:lower			C805	JAD06150Q6D	IOS 12.1(5)YB5	
Winchester:HQ:MainRack:Cisco 2924xl s			C2900XL	FOC0508Z37G	IOS 12.0(5)WC9a	
Winchester:B3-1:Gnd:UPS-rack			Catalyst 5000/5500 Switch	069028540	CatOS 5.5(12)	1 WS-X5509 (2) 7409318 3 WS-X5203 (12) 6840528 4 WS-X5302 (1) 8701649 5 WS-X5225R (24) 13385899 6 WS-X5201R (12) 13154875 8 WS-X5224 (24) 10109808 9 WS-X5225R (24) 13390939 10 WS-X5203 (12) 7418254 11 WS-X5224 (24) 10445812 12 WS-X5302 (1) 8689596
Unknown	10.100.10.97	demo.eagle-eyes.co.uk	Linux	Unknown	Linux 2.6.9-34.106.unsupportedsmp	
Winchester:Remote_Office:Cabinet:HP 2626 switch	159.60.76.199	Depot-HP2626	HP 2626-PWR	Unknown	HP sw:H.07.41 ,	
Unknown	10.100.10.89	Depot-HP2626(000e7f-a36140)	HP 2626-PWR	Unknown	Revision H.07.41 /sw/code/build/fish(ff03)	
Winchester:HQ:MainRack:Cisco803	10.100.10.100	phine-home	C800	JAD04200FE5 (2703055633)	IOS 12.2(3)	
Winchester:HQ:Lab	192.168.15.4	RSM-honeycut	C5RSM		IOS 12.2(23)	
Sandhurst:1CP:Ground:Computer Room	192.168.0.206	S1-1_2610_Picard.haqa.co.uk	C2600	JAD05060TKX (3187103671)	IOS 12.0(28d)	
Sandhurst:1CP:Ground:Computer Room	192.168.0.251	S1-1_450-24T_Guinan	Unknown	Unknown	Bay fw:v1.36 sw:1.3.1.2	
Unknown	10.100.10.101	SEP0013C427F09A	Cisco IP Phone 7902	Unknown	CP7902-v1-03-0-040312B	
Unknown	192.168.0.9	SEP003094C43051	Cisco IP Phone 7960	Unknown	P00308000300	

Unit Name: B1-1_2610_Winchester
Location: Winchester:HQ:LabRack1:Cisco 2610 at top
Address: 192.168.17.2
Model: C2600
Serial No.: JAD05060E2N (819268478)
Running For: 617h 19m 06s

This unit is connected to:

Local Port	Remote Unit	Remote Port
Tunnel0	S1-1_2610_Picard.haqa.co.uk	Tunnel0
Serial0/0	B1-1_2611_Stacey	Serial0/0

Syslog server – providing a central repository for all logged error messages from the networking infrastructure; logs are auto-archived and rotated monthly; all viewable from the web interface.

TFTP server – hold your software images in one place, alongside all of your network infrastructure configuration files. View these (password-protected) via the web browser.

ConfigWatch (future) – get infrastructure configurations regularly and check against the last known config; highlight any changes; major changes are provided as an alert (email or SMS).

Auto-map (future) – groups devices by location, providing automatic maps showing connection by key network links.

Storm Detect (future) – analyses broadcast levels passing the appliance, generating a baseline of "normal" activity – alerting when levels exceed this or when unexpected devices broadcast on the network.

About Hinx Limited

Our clients use Hinx Limited because we are recognized as experts in our field. Our expertise is in design and implementation of complex data and voice networks, utilising modern Quality of Service mechanisms to deliver to clients' expectations.

Hinx have two full-time consultants, each of whom hold the highest networking accreditation, Cisco Certified Internetworking Expert. This qualification takes time and dedication to achieve, as well as the all-important experience. Both consultants worked for Cisco for over 8 years, and together they have 30+ years of data communications and 7 years of voice communications experience.

Here's what our clients have to say about us:

> *"Hinx have never let us down and have the expertise we need",* IT & Network Manager, Windrush Frozen Foods Limited
>
> *"Their standard of documentation is impeccable – which makes a real difference to the standard of support we receive",* IT Manager, Raymarine UK PLC
>
> *"The project ran really smoothly – [Hinx] arranged everything for us",* IP & Data Architecture Manager, Cable & Wireless PLC.

For more details of any of Hinx services, consult our website http://www.hinx.com, call our sales office on 01962 886 174 or email sales@hinx.com