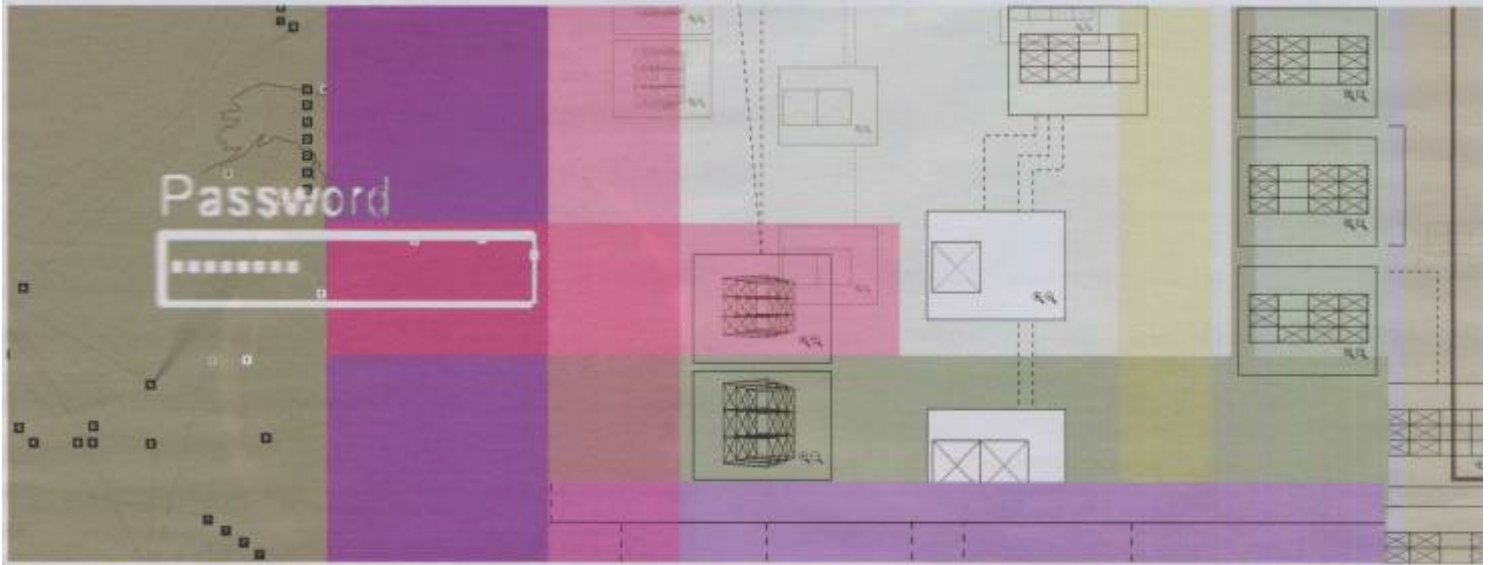




FUTURE TRENDS The dream of a self-sufficient network is growing closer to realisation. The key challenge is to integrate self-healing capabilities at every layer of the operation

Helping the network to take control of itself



Blueprint for darkroom network operations: will network managers ever be able to go home without having to worry about a crash in the computing infrastructure?

Danny Bradbury
computer.weekly@rbi.co.uk

For IT departments, the concept of darkroom operation can have one of two meanings. Ideally, it means a computing infrastructure that lets you turn off the lights and go home without worrying about it crashing. It is a nice idea, but for most systems administrators and network managers, the second meaning is all too prevalent - their networks make them want to crawl into a dark room and stay there.

For a network to be truly self-sufficient, it must be self-healing. Developing a computer network that fixes its own problems, maintaining service levels in the face of unpredictable operating conditions, is no mean feat. Compounding the problem is that for a network to be truly autonomous it has to have self-healing capabilities at all levels of the stack, not just the routing and switching layers.

Other things to consider are application management, so software can be programmed to cope with failure, and security. With threats to corporate networks increasing, security is one of the biggest service disrupters facing the industry.

At the lower levels of the seven-layer OSI model of a network infrastructure, the self-healing of physical network problems may not be possible. If a physical cable breaks, someone has to go

Topology discovery can help discover the shape of a local area network that is experiencing problems and compare it to a picture of the network before the problem arose, so that error messages can be more descriptive

and fix it. "There are no robots to fix a circuit when its soldering cracks apart," said Rami Houby, European business development director at switch supplier Allied Telesyn. "You have to send someone out." This is true, but there are some technologies you can use even at this level - or may be able to use in the future.

One useful ability for any network that is trying to heal itself is to know what its own topology is. Traditionally, high-end management systems such as HP Openview rely on the Simple Network Management Protocol (SNMP) to discover equipment on the network, storing the information in a Management Information Base (MIB). This is all very well, but what about users in smaller companies without these resources, or a branch office?

"Imagine a scenario such as a small firm with no dedicated IT staff," said Richard Black, researcher at Microsoft Research Cambridge. "If someone kicks a power cable out from a device and people suddenly have no e-mail, they do not know whether it is an application failure, a hardware failure or a connection problem." Topology discovery can help discover the shape of a local area network that is experiencing problems and compare it to a picture of the network before the problem arose, so that error messages can be more descriptive. Black has been working on a protocol that enables networks to au-

tomatically discover their own topologies without resorting to SNMP and MIB software. His research uses a topology discovery protocol that works at the media access control layer underneath the IP address layer.

A PC is used to instruct all other enabled devices to begin querying the network, finding as many devices as they can. This information is then reported back to the controlling PC and a picture of the network is built. Although the technology has not been turned into a product yet, it could yield results in the future. It might not make the network completely self-healing, but it may at least help non-technical local staff solve the problem without bringing down the boys from head office.

In the meantime, existing technologies such as the IEEE's spanning tree protocol (STP) are also being used to increase network resilience at layer two of the OSI stack (the data link layer, which handles data transmission but sits underneath the IP address layer). STP works by automatically turning off redundant links on a network, where multiple connections exist between two devices. If such links are left active, data storms can occur where packets are repeatedly transmitted for no reason. Should the remaining links experience problems, STP, which uses a heartbeat mechanism to keep querying the status of the network, can be used to

bring up the original links to keep communication flowing.

Such technologies work well in a Lan environment, but what about in a Wan? Because of the IP-based routing needed to make Wan communications work, the solutions move further up the networking stack. One relevant technology here is the Virtual Router Redundancy Protocol (VRRP), which allows a collection of physical routers to be viewed as one virtual router. Should one router fail, another one can step up to take its place, transparently to the applications communicating across the network.

But routers that replace other routers are not enough. Often, network health is not simply a binary affair in which a piece of equipment is either alive or dead. But what if it is sick or under attack? In this case, smarter solutions are needed. Traffic shaping suppliers such as Packeteer have traditionally sold products that impose relatively static rules on traffic flow, throttling some applications such as peer-to-peer networks while allowing more throughput to others such as VoIP.

The company recently launched its adaptive response technology, which will be included in all future updates to its products distributed around a customer's network. It monitors network conditions and adjusts
→ continued on p52



← continued from p50

its traffic rules to respond to them. If, for example, a particular port on a server was being uncharacteristically pounded by incoming packets, Packeteer could throttle back the suspicious traffic automatically until the problem could be further investigated.

Such security concerns are at the forefront of initiatives from Cisco, Microsoft and IBM. These suppliers are concerned about the network's vulnerability to connections from compromised clients. Cisco's self-defending network initiative is a strategy designed to produce self-configuring networks that block attacks, according to senior security consultant Paul King.

The company has concentrated on plugging security into the "endpoints" – the desktop PCs and servers – on the network, as well as into the firewalls by giving customers the option to install its Cisco security agent behaviour analysis software on these network nodes.

Meanwhile, the company is beginning to deliver some parts of its network admission control (NAC) strategy, which uses a Cisco trust agent (CTA) – a client-based software agent enabling Cisco's access control server to query client operating systems. So, when a client connects to the network, the network can ensure it has the latest operating system patches and virus updates before it is allowed full access.

"The network can decide whether an endpoint is compliant and quarantine it if it is not," King said. "The NAC programme is about developing the APIs so that the access control server can then talk to the various anti-virus policy servers."

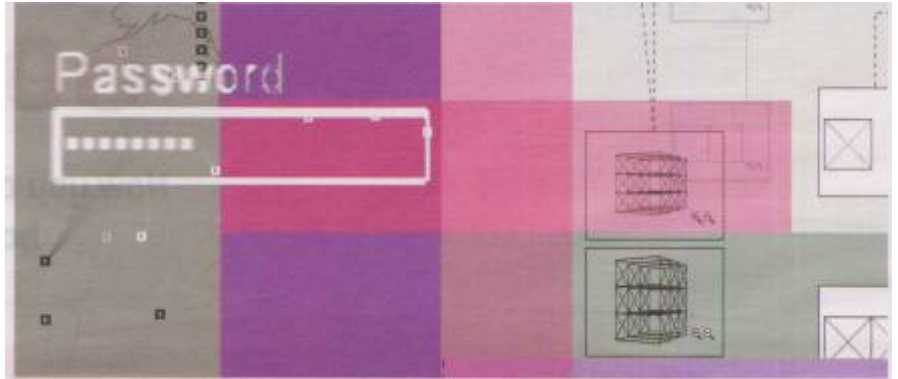
Policy definitions are an important part of the equation, enabling network managers to define rules governing the treatment of a compromised PC. Cisco is relying on third-party partners to layer extra functions on top of the network access control technology.

One example could be an enhancement of its existing intrusion detection system (IDS), King suggested. "When it sees a packet go by, and identifies it as a Code Red worm packet, rather than signalling an alarm, why doesn't the IDS find out what server and program the packet was destined for, and then check that the software has been patched? When you start doing this, you are starting to get into self-defending networks."

Fortunately, Cisco has decided to work with Microsoft, which is preparing its own client compliance technology that will ship in a Windows 2003 server update next year. At least customers will not have to spend time trying to integrate the two.

Another alliance partner is

The system will not only make a diagnosis and produce a recommendation, but it will also carry out that recommendation on its own



IBM Tivoli, which has integrated its identity management capabilities into the Cisco access control server, said Peter Jopling, IBM Tivoli's head of security, EMEA. The latest phase of its integration involves understanding who is connected to the network and what they have on their machines. "If when they connect to the network it does not meet the corporate requirements, we hold them on a part of the Lan and update the machine before letting them connect to the rest of the network," he said.

The roll-out of NAC technology within Cisco's products has been relatively limited. For example, only routers are currently NAC-enabled to query where endpoints were when they connect to the network. Cisco switches will be NAC-enabled at a later date, said King. Consequently, IBM took the decision to integrate directly with Cisco's access control server, leaving NAC out of the equation, said Jopling.

Moving still further up the stack, some companies are focusing on the applications themselves. Even if your network is operating relatively autonomously at lower levels, if an application fails, the effects on the business will be much the same.

Motive is an application configuration company selling a suite of products designed to diagnose an application's state automatically, based on an application definition model – essentially a snapshot of what an application configuration should look like. This serves as a reference point for automated investigation and diagnosis. "We model once and then analyse any time and anywhere, encapsulating constraints into the model in the form of restraints and dependencies," said Jay Hallberg, vice-president of product marketing and management for the company. "We use the concept of a known working state."

Hallberg said the system focuses mostly on diagnosing system problems and making recommendations to IT personnel because the level of trust in com-

pletely automatic remediation is still relatively low among IT staff. "We dialled the product back and suppressed the autonomic capabilities because people just want to see it run for a while," he said.

Nevertheless, customers wishing to throw caution to the wind can turn these facilities on in the software. It will then not only make a diagnosis and produce a recommendation, but also carry out that recommendation on its own.

To take an example, Hallberg says that one application server in one of his customer's infrastructures must allow a number of application threads to run, to avoid becoming unstable and rendering the applications running on it unresponsive.

Owing to an architectural limitation, after a certain volume of transactions the application server resets the threading mechanism and scripts built into the system notify the system administrator to take action. Motive can use its product to automate the whole

process, removing this human interaction from the equation.

Another, a simple example, could involve automating software restarts if a critical part of an application fails.

One of the biggest problems for companies trying to increase the autonomy of their network is the integration of these different layers of the stack. Few companies, if any, claim to offer all parts of the solution. "I think that needs to happen at the top level," said Jeff Barker, director of product marketing at Packeteer, "at the level of the management consoles offered by IBM Tivoli and Hewlett-Packard."

Given various disciplines that must be pulled together to make this viable – everything from load balancing through to security and application profiling – it will take a supplier with deep pockets to pull it all together into one easily digestible package. In the meantime, most IT departments will find themselves fighting fires for the foreseeable future.

Networking acronyms

- **SNMP:** Simple Network Management Protocol, used to discover equipment on the network
- **MIB:** management information base, used for storing the information
- **NAC:** network admission control, part of Cisco's self-defending network strategy, which uses a Cisco trust agent (CTA) – a client-based software agent enabling Cisco's access control server to query client operating systems

- **IDS:** intrusion detection system
- **ADM:** application definition model – essentially a snapshot of what an application configuration should look like
- **OSI Seven Layer Model for Network Architecture:** one of the biggest problems for companies trying to increase the autonomy of their network is the integration of these different layers of the stack. Few companies, if any, claim to offer all parts of the solution.

OSI Seven Layer Model

The Open Systems Interconnection (OSI) Seven Layer Model for Network Architecture:

- **Seven:** application. Provides different services to apps
- **Six:** presentation. Converts the information
- **Five:** session. Handles problems which are not communication issues

- **Four:** transport. Provides communication control
- **Three:** network. Routes information in the network
- **Two:** data link. Provides error control between adjacent nodes
- **One:** physical. Connects the entity to the transmission media.