Autonomic networking

From Wikipedia, the free encyclopedia

Autonomic Networking follows the concept of Autonomic Computing, an initiative started by IBM in 2001. Its ultimate aim is to create self-managing networks to overcome the rapidly growing complexity of the Internet and other networks and to enable their further growth, far beyond the size of today.

Contents

Increasing size and complexity

The ever-growing management complexity of the Internet caused by its rapid growth is seen by some experts as a major problem that limits its usability in the future.

What's more, increasingly popular smartphones, PDAs, networked audio and video equipment, and game consoles need to be interconnected. Pervasive Computing not only adds features, but also burdens existing networking infrastructure with more and more tasks that sooner or later will not be manageable by human intervention alone.

Another important aspect is the price of manually controlling huge numbers of vitally important devices of current network infrastructures.

Autonomic nervous system

The autonomic nervous system (ANS) is the part of the nervous system of the higher life forms that is not consciously controlled. It regulates bodily functions and the activity of specific organs. As proposed by IBM, future communication systems might be designed in a similar way to the ANS.

Components of autonomic networking

As autonomics conceptually derives from biological entities such as the human autonomic nervous system, each of the areas can be metaphorically related to functional and structural aspects of a living being. In the human body, the autonomic system facilitates and regulates a variety of functions including respiration, blood pressure and circulation, and emotive response. The autonomic nervous system is the interconnecting fabric that supports feedback loops between internal states and various sources by which internal and external conditions are monitored.

Autognostics

Autognostics includes a range of self-discovery, awareness, and analysis capabilities that provide the autonomic system with a view on high-level state. In metaphor, this represents the perceptual sub-systems that gather, analyze, and report on internal and external states and conditions – for example, this might be viewed as the eyes, visual cortex and perceptual organs of the system. Autognostics, or literally "self-knowledge", provides the autonomic system with a basis for response and validation.

A rich autognostic capability may include many different "perceptual senses". For example, the human body gathers information via the usual five senses, the so-called sixth sense of proprioception (sense of body position and orientation), and through emotive states that represent the gross wellness of the body. As conditions and states change, they are detected by the sensory monitors and provide the basis for adaptation of related systems. Implicit in such a system are imbedded models of both internal and external environments such that relative value can be assigned to any perceived state - perceived physical threat (e.g. a snake) can result in rapid shallow breathing related to fight-flight response, a phylogenetically effective model of interaction with recognizable threats.

In the case of autonomic networking, the state of the network may be defined by inputs from:

- individual network elements such as switches and network interfaces including
  - specification and configuration
  - historical records and current state
- traffic flows
- end-hosts
- application performance data
- logical diagrams and design specifications

Most of these sources represent relatively raw and unprocessed views that have limited relevance. Post-processing and various forms of analysis must be applied to generate meaningful measurements and assessments against which current state can be derived.

The autognostic system interoperates with:

- configuration management - to control network elements and interfaces
- policy management - to define performance objectives and constraints
- autodefense - to identify attacks and accommodate the impact of defensive responses

Configuration management

Configuration management is responsible for the interaction with network elements and interfaces. It includes an accounting capability with historical perspective that provides for the tracking of configurations over time, with respect to various circumstances. In the biological metaphor, these are the hands and, to some degree, the memory of the autonomic system.

On a network, remediation and provisioning are applied via configuration setting of specific devices. Implementation affecting access and selective performance with respect to role and relationship are also applied. Almost all the "actions" that are currently taken by human engineers fall under this area. With only a few exceptions, interfaces are set by hand, or by extension of the hand, through automated scripts.

Implicit in the configuration process is the maintenance of a dynamic population of devices under management, a historical record of changes and the directives which invoked change. Typical to many accounting functions, configuration management should be capable of operating on devices and then rolling back changes to recover previous configurations. Where change may lead to unrecoverable states, the sub-system should be able to qualify the consequences of changes prior to issuing them.

As directives for change must originate from other sub-systems, the shared language for such directives must be abstracted from the details of the devices involved. The configuration management sub-system must be able to translate unambiguously between directives and hard actions or to be able to signal the need for further detail on a directive. An inferential capacity may be appropriate to support sufficient flexibility (i.e. configuration never takes place because there is no unique one-to-one mapping between directive and configuration settings). Where standards are not sufficient, a learning capacity may also be required to acquire new knowledge of devices and their configuration.

Configuration management interoperates with all of the other sub-systems including:

- autognostics - receives direction for and validation of changes
- policy management - implements policy models through mapping to underlying resources
- security - applies access and authorization constraints for particular policy targets
- autodefense - receives direction for changes

Policy management

Policy management includes policy specification, deployment, reasoning over policies, updating and maintaining policies, and enforcement. Policy-based management is required for:

- constraining different kinds of behavior including security, privacy, resource access, and collaboration
- configuration management
- describing business processes and defining performance
- defining role and relationship, and establishing trust and reputation

It provides the models of environment and behavior that represent effective interaction according to specific goals. In the human nervous system metaphor, these models are implicit in the evolutionary "design" of biological entities and specific to the goals of survival and procreation. Definition of what constitutes a policy is necessary to consider what is involved in managing it. A relatively flexible and abstract framework of values, relationships, roles, interactions, resources, and other components of the network environment is required. This sub-system extends far beyond the physical network to the applications in use and the processes and end-users that employ the network to achieve specific goals. It must express the relative values of various resources, outcomes, and processes and include a basis for assessing states and conditions.

Unless embodied in some system outside the autonomic network or implicit to the specific policy implementation, the framework must also accommodate the definition of process, objectives and goals. Business process definitions and descriptions are then an integral part of the policy implementation. Further, as policy management represents the ultimate basis for the operation of the autonomic system, it must be able to report on its operation with respect to the details of its implementation.

The policy management sub-system interoperates (at least) indirectly with all other sub-systems but primarily interacts with:

- autognostics - providing the definition of performance and accepting reports on conditions
- configuration management - providing constraints on device configuration
- security - providing definitions of roles, access and permissions

Autodefense

Autodefense represents a dynamic and adaptive mechanism that responds to malicious and intentional attacks on the network infrastructure, or use of the network infrastructure to attack IT resources. As defensive measures tend to impede the operation of IT, it is optimally capable of balancing performance objectives with typically over-riding threat management actions. In the biological metaphor, this sub-system offers mechanisms comparable to the immune system.

This sub-system must proactively assess network and application infrastructure for risks, detect and identify threats, and define effective both proactive and reactive defensive responses. It has the role of the warrior and the security guard insofar as it has roles for both maintenance and corrective activities. Its relationship with security is close but not identical – security is more concerned with appropriately defined and implemented access and authorization controls to maintain legitimate roles and process. Autodefense deals with forces and processes, typically malicious, outside the normal operation of the system that offer some risk to successful execution.

Autodefense requires high-level and detailed knowledge of the entire network as well as imbedded models of risk that allow it to analyze dynamically the current status. Corrections to decrease risk must be considered in balance with performance objectives and value of process goals – an overzealous defensive response can immobilize the system (like the immune system inappropriately invoking an allergic reaction). The detection of network or application behaviors that signal possible attack or abuse is followed by the generation of an appropriate response – for example, ports might be temporarily closed or packets with a specific source or destination might be filtered out. Further assessment generates subsequent changes either relaxing the defensive measures or strengthening them.

Autodefense interoperates closely with:

- security - receives definition of roles and security constraints, and defines risk for proactive mitigation
- configuration management - receives details of network for analysis and directs changes in elements in response to anticipated or detected attack
- autognostics - receives notification of detected behaviors

It also may receive definition of relative value of various resources and processes from policy management in order to develop responses consistent with policy.

Security

Security provides the structure that defines and enforces the relationships between roles, content, and resources, particularly with respect to access. It includes the framework for definitions as well as the means to implement them. In metaphor, security parallels the complex mechanisms underlying social interactions, defining friends, foes, mates and allies and offering access to limited resources on the basis of assessed benefit.

Several key means are employed by security – they include the well-known 3 As of authentication, authorization, and access (control). The basis for applying these means requires the definition of roles and their relationships to resources, processes and each other. High-level concepts like privacy, anonymity and verification are likely imbedded in the form of the role definitions and derive from policy. Successful security reliably supports and enforces roles and relationships.

Autodefense has a close association with security – maintaining the assigned roles in balance with performance exposes the system to potential violations in security. In those cases, the system must compensate by making changes that may sacrifice balance on a temporary basis and indeed may violate the operational terms of security itself. Typically the two are viewed as inextricably intertwined – effective security somewhat hopefully negating any need for a defensive response. Security's revised role is to mediate between the competing demands from policy for maximized performance and minimized risk with auto defense recovering the balance when inevitable risk translates to threat. Federation represents one of the key challenges to be solved by effective security.

The security sub-system interoperates directly with:

- policy management - receiving high-level directives related to access and priority
- configuration management - sending specifics for access and admission control
- autodefense - receiving over-riding directives under threat and sending security constraint details for risk

assessment

Connection fabric

The connection fabric supports the interaction with all the elements and sub-systems of the autonomic system. It may be composed of a variety of means and mechanisms, or may be a single central framework. The biological equivalent is the central nervous system itself – although referred to as the autonomic system, it actually is only the communication conduit between the human body's faculties.

Principles of autonomic networking

Consequently, it is currently under research by many research projects, how principles and paradigms of mother nature might be applied to networking.

Compartmentalization

Instead of a layering approach, autonomic networking targets a more flexible structure termed compartmentalization.

Function re-composition

The goal is to produce an architectural design that enables flexible, dynamic, and fully autonomic formation of large-scale networks in which the functionalities of each constituent network node are also composed in an autonomic fashion

Atomization

Functions should be divided into atomic units to allow for maximal re-composition freedom.

Closed control loop

A fundamental concept of Control theory, the closed control loop, is among the fundamental principles of autonomic networking. A closed control loop maintains the properties of the controlled system within desired bounds by constantly monitoring target parameters.

See also

- Autonomic Computing
- Autonomic system (computing)
- Cognitive networks
- Network Compartment
- The Autonomic Network Architecture (ANA) Project
- Collaborative innovation network

- In-Network Management
- Generic Autonomic Networking Architecture (GANA) EFIPSANS Project http://www.efipsans.org/

External links

- IBM Autonomic Computing Website (http://www.ibm.com/autonomic)
- Intel White Paper: Towards an Autonomic Framework (https://web.archive.org/web/20080224033918/http://download.intel.com/technology/itj/2004/volume08issue04/art03_autonomic/vol8_art03.pdf)
- Ipanema Technologies: Autonomic Networking applied to application performance optimization (http://www.ipanematech.com)

Research projects

- ANA Project: Autonomic Network Architecture (http://www.ana-project.org/)
- ANAPORT is an open bibliography reference developed within the ANA project (http://www.ana-project.org/ref/)
- Beyond-The-Horizon: Coordination Action by the European Commission (http://www.beyond-the-horizon.net/)
- Bionets: Biologically-inspired concepts for networking (http://www.bionets.eu/)
- BiSNET: Biologically-inspired architecture for Sensor NETworks (http://dssg.cs.umb.edu/wiki/index.php/BiSNET)
- BiSNET/e: A Cognitive Sensor Networking Architecture with Evolutionary Multiobjective Optimization (http://dssg.cs.umb.edu/wiki/index.php/BiSNET/e)
- Component-ware for Autonomic Situation-aware Communications, and Dynamically Adaptable Services (https://web.archive.org/web/20060527201638/http://www.cascadas-project.org:80/)
- Diet Agents: Indefinitely scalable hosting for systems of autonomic interacting processes (http://diet-agents.sourceforge.net)
- EFIPSANS Project: Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building autonomic Networks and Services (http://efipsans.org/)
- Haggle: An innovative Paradigm for Autonomic Opportunistic Communication (http://www.haggleproject.org/)
- SOCRATES: Self-Optimization and Self-Configuration in Wireless Networks (http://www.fp7-socrates.org/)
- Dynamically Self Configuring Automotive System (http://www.dyscas.org)
- Self-NET: Self-Management of Cognitive Future InterNET Elements (http://ict-selfnet.eu)
- AutHoNe: Autonomic Home Networking (http://www.authone.de)
- SymbioticSphere: A Biologically-inspired Architecture for Scalable, Adaptive and Survivable Network Systems (http://dssg.cs.umb.edu/wiki/index.php/SymbioticSphere)
- TRANS: TRANS demonstrate a tightly integrated network and service overlay architecture with advanced traffic-aware and self-organisation functionality (http://projects.celtic-initiative.org/trans/)
- UniverSELF project: Realising autonomics for Future Networks (http://www.univerself-project.eu:)

Blogs and Wikis

- Autonomic Networking Wiki: A wiki dedicated to Autonomic Networking (https://web.archive.org/web/20081121035631/http://www.autonomicnetworking.org/)

- Autonomic networking at the core of enterprise Wan governance blog (https://web.archive.org/web/20090531083332/http://www.wan-governance.com:80/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Autonomic_networking&oldid=745619365"

Categories: Artificial intelligence | Information technology management | Information technology governance | Network management | Wide area networks | WAN optimization | Network performance

---