Traditionally, a network is built around physical locations and with a “hard” exterior (firewalls, remote access mechanisms, etc.) Typically, networks tend to be static - primarily because it is difficult to make networks dynamic and because physical locations change infrequently. A network is usually configured using routers; these routers may be configured to enforce some network security via ACLs – Access Control Lists. Firewalls configurations often use ACLs.

What issues arise in the traditional network?

Network changes and reconfigurations are difficult since every network component needs to be managed separately. Changes and reconfigurations of network devices are quasi-exclusively performed manually. This leads to flexibility problems, cost, and errors which in turn to security and service level problems.

Users in one physical location don’t necessarily work for the same organization and may be working under different security policies. When a company has partners or suppliers with network connections into the organization, this is typically managed is via gateways for external partners and through identity management systems for internal partners.

Change is a slow process — reconfiguring a network can take weeks or months if the network is worldwide.

New business models can be difficult to implement

What is ANA (Adaptive Network Architecture)?

ANA takes the view that a more flexible architecture would have a virtual backbone (that is, IP transport only) to which user groups can be attached. The user groups (compartments) contain users with the same access rights and security policy. A compartment however is not necessarily a physical location. For example, if users in London have the same function as a group in New York, they can be grouped and managed as though they existed together on the same private sub-network. The following graphic demonstrates this idea:
What are the advantages of ANA?

- Flexibility — compartments are managed centrally and reconfiguration of the network for business or security reasons are done faster, and in a very controlled and secure way. Instead of taking weeks to update policy rules, the same activity can be done in matter of hours.
- Security — users can be grouped according to policy and not location. Therefore, auditing is easier.
- Cost — reconfiguration is fast and centralised.
- Because the Virtual Backbone is dissociated from the user compartments, it can be managed separately and evolve separately in line with the most cost-effective transport means and eventually become the organization’s Internet.

How is it done?

HP’s Policy Registry Tool that allows a central point to define and check the integrity of policies and then to roll these out via ACL updates to all involved network components.
HP always performs a review of the desired architecture using ITSA (IT Solution Architecture) methodology and an ROI calculation to ensure that the future state satisfies the customer's needs and is worth doing. In practice, we would usually 'compartmentalize' one group of users or an application at a time.

Examples:

- A company has desktop machines, some of which are not secure. When one of these machines logs on, they would be placed in a different compartment with restricted access.

- A company has a single site where some parts of policy are not implemented. This site — or part of the site — would be placed into a different compartment.

- A company has partners with some of those as development partners. The developers of both companies would be placed into a single compartment (as HP did with Intel).

- A company has different access rules for sales and support. These would be placed in different network compartments regardless of their physical location.

- A company has no hard or defined barrier where it can put a firewall — roaming end-users with differing devices is an example.

Who has the problem?

Customers with multiple sites, international sites, multiple partners or suppliers. Any client where rapid change or divestiture or acquisition is occurring.

HP and Cisco Partnership

Identity Based Networking from Cisco is essentially 802.1x. This follows the idea that a machine is authenticated at Level 2 before it is allowed access to the network. HP and Cisco have jointly created AIBN which is the combination of ANA and IBNS. AIBN gives our customers the ability to quickly deploy more secure, global network compartments with user-based access control that allows IT to meet ever-changing business needs.

Can you do this manually?

On a large network is impossible to do in a reasonable time and accurately. Having to deploy the same rules several times in different geographic dispersed network components, makes the amount of policies larger and very complex to manage. With ANA, the number of ACLs (access control lists) decrease dramatically and can be provisioned automatically, in a centralized manner, no matter what location the network component is. As a simple example, deploying the Intel/HP relationship with ANA involved deploying 300 ACLs — without ANA the number would have been closer to 30,000.