

Happy Network Administrators Lead to Happy Users!

Position Statement

Workshop on Internet Routing Evolution and Design (WIRED), October 2006

Aman Shaikh

*AT&T Labs – Research
Florham Park, NJ 07932
ashaikh@research.att.com*

Why Care About Network Administrators?

Network administrators and operators want to run their networks well so that their customers are happy! Running a network is supposed to be simple. After all, the core was designed to be simple and all the complexity was supposed to lie at the edge. Unfortunately, network core is incredibly complex now. The scale alone is bewildering, but what makes things even more complicated is that networks are often spread over vast geographical areas and run myriad of protocols that evolve all the time. Furthermore, the Internet that was designed for best effort traffic now carries traffic for real-time applications such as voice, video and gaming. All this has made network administrators' task enormously challenging.

What further exacerbates things is that IP networks do not have much management support built into them except for SNMP, syslog and NetFlow – which are often inadequate. And nowhere this lack of support is felt more acutely than at the routing layer. Consider this basic question that any network administrator is likely to ask: “what path did traffic take from router A to router B in my network some x hours ago?” Answering this question is often impossible since it requires historical routing information from several routers in the network and coalescing this information.

Luckily, research community has started paying attention to network management issues. Several papers dealing with new management paradigms, new control plane architectures, management tools and control plane anomaly detection have appeared in various research forums over last few years. However, a lot needs to be done if we want to achieve the holy grail of complete automation of network management.

What Can Researchers Do?

So what can we researchers do to improve the state-of-the-art of network management? In my opinion, following are some areas that need to be addressed:

- **Configuration Management:** Configuring routers and other devices in the network is one of the biggest headaches for network administrators. First of all, configuration commands are often primitive yet at the same time complicated and un-intuitive. The command interface should provide right amount of abstraction and flexibility for operators to easily but precisely express their intent. Second, network configuration happens on a device-by-device fashion. We need to move away from such device-level configurations to network-level configuration. This requires languages for expressing network-level intent, and tools for translating this intent into per-device configuration. Third, routers have plethora of configurable parameters and tunable knobs, and the number keeps increasing every day. Yet, setting appropriate values for these parameters is challenging. Defaults often do not make sense either because they are arcane or there are no one-size-fits-all values. This forces operators to resort to intuition and tweak-and-pray methods. The challenge for us then is how to make setting of configurable parameters

a science. Going a bit further, can we design systems that can adaptively set and change the settings based on performance goals and observed state of the network?

- **Network Trouble-shooting:** Finding the root cause when something goes wrong in a network and fixing it is always a painful task. There are several reasons for this. First, determining what is in a “router’s mind” (*i.e.*, control plane intelligence) is not easy. SNMP and syslog do not provide enough information. Plus they are not reliable — especially during failures! Route monitors (that collect routing updates by peering with routers or through some other means) have filled some of this gap, but deploying them requires careful engineering procedures to ensure they do not adversely impact the routers. What administrators really need is “passive sessions” over which route updates and other routing related information can be collected with minimal impact on the functioning of the routers. Second, even when we collect routing messages, they do not carry any information about the root cause. This means we either need to modify protocols to supply this information or design tools that can allow us to infer root cause reliably, effectively and scalably from the routing messages. Third, routing protocols are designed with isolation in mind, yet in practice they interact with one another, and often in strange ways. We need better isolation of protocols. Yet when the protocols do interact, we need to model the interactions in a way that eases trouble-shooting. Finally, for failures that occur over a course of time in a gradual manner, we need tools and methods to detect them as early as possible, and if possible even predict them.
- **Network Maintenance:** Seamlessly performing maintenance and upgrade of the routing infrastructure is another task that administrators grapple with all the time. Several network melt-downs have occurred as undesirable side-effects of network upgrades. It is imperative that we find ways to make these upgrades as seamless and pain-free as possible by changing protocols (*e.g.*, by adding graceful restart mechanisms), and by designing routers that can be upgraded while in service. Scheduling upgrades also gets challenging for large networks with huge customer base since operators have to ensure that customer impact is minimized while at the same time they have to satisfy the constraints imposed by operational procedures and take into account the inter-dependency of network devices. Scheduling has of course been a well explored area, but what has not been explored is how to gauge the effect of a planned maintenance/upgrade on data traffic and end users. Finally, we also need to find ways for operators to safely back out of a maintenance procedure should things go bad.
- **Network Security:** Control plane security is a critical issue, especially for the inter-domain routing. BGP security problems are well known, quite a few solutions have been proposed, but hardly anything has happened in terms of deployment. Why? As researchers, we really need to find ways of *incrementally* beefing up the control plane security. To me, that is the single biggest challenge when it comes to security.

In closing, let us make life easier for the network administrators who toil day and night to keep our networks humming. Because happy administrators lead to happy end users!