Technical Summary

- R.Ranjan (CS12B050)

Active Networking

Aim:
The aim of active networking is to bring programmability to the lower layers of the networking world. The idea is to enable programmability by the use of transferring control to the packet themselves.

Implementation:
The novelty of the idea lies in the fact that it has the potential to increase the speed of research in the networking field and the easy modification to the existing systems. Basically, it is like a packet containing a code which would be loaded onto a router which would then use the program on the packet to modify the functions of the router or decide the fate of the current packet itself. Not all packets should be like these as it might end up slowing down the system. These are special packets called active packets. The active networking system consists of a node operating system and an execution environment. The OS should be able to handle one or more execution environments. It also should contain active hardware capable of routing, switching and execution when it comes to active packets.

Innovation:
This breaks away from traditional networks because if this comes into play, the robustness and the propriety of a router would be compromised which is a reason as to why it faces promotional hindrance from companies like CISCO.

Theoretical challenges:
Unlike computers came into existence based on the fundamental theoretical idea of turing machines, the mathematical theoretical framework from information theory is not exactly understood. Therefore fundamental research in information theory regarding this is essential for proper advancement in active networking.

Other Challenges:
The average time which is required to process one packet of 40 bytes is 3.2 ns.
Hence the first consideration is the potential complexity involved in creation of the routers which could potentially slow down the network. As the theoretical framework is not yet robust, we don’t exactly know the ideal number of control packets per 1000 other packets or such.

Future Advancements;
The use of AI in networking field can be enabled by active networking by the introduction of genetic algorithms which is a search heuristic based on simulating natural selection.
Active networking hence allows the possibilities of rapid changes to the underlying network.

IETF ForCES

Motivation:
There are two main elements in a network situation namely control element and forwarding element or the data element. Currently the information exchange between the two elements is generally proprietary. This is a big hindrance for large systems because they have to stick to one particular company. Therefore replacement of a particular element is forced to be from a different manufacturer. Combination of two best equipments seems really hard. As of now new manufacturers are simply blocked because of the inoperability and the wholesome service which they need to provide.

Aim:
ForCES stands for Forwarding and Control Element Separation. This is a standard for implementing control plane and data plane. ForCES aims to define a framework and associated protocol(s) to standardize information exchange between the control and forwarding plane.

Implementation:
It is done by the presence of several logical functional blocks called LFBs. One forwarding element could potentially contain multiple LFBs. LFBs are defined using inputs, outputs and different components that can be configured in the LFB by the Control Element. There can be multiple instances of the same functionality required in a setup. So for identification of an LFB the key we have is the LFB Class ID. The control element is made to be able to work with any data path from different vendors if the LFBs which the vendors have to develop are as per the IETF standard.

General Advantages:
This implies that interoperation between devices of different manufacturers becomes possible and also opens a new field of manufacturers who can specialize in just one component. This enhances the possibility of rapid innovation in both the elements without bothering about the communication between the two. Scalability is also supported by this methodology. Basically if the communication is standardized, the communication is no more a specialty and no longer linked more to the different fields of controlling and forwarding elements. This process, even though doesn’t completely separate the two elements, provides considerable structure to the data path.

Implementation specific advantages:
Forces follows the ‘type’, ‘length’ and ‘value’ methodology or what is known as TLV in its header for messages transferred between the two elements which can work like the options header which we have seen in TCP, etc. Though this does consists of sending more data, in future it might be helpful for specific processing, etc. The implementation of tables is upto the LFB, unlike the Openflow which forces exact match tables, so long as the outside behaviour is the same.

Routing Control Platform

Motivation:
The current systems have BGP implemented at various gateways. These are extremely configurable and hence tough to understand and are present in abundance. The diagnosis of these BGPs becomes extremely complex because of the above reasons. It is also very hard to even predict how a system might behave after a few configurational changes.

Aim:
The routing control platform aims to compute the border gateway protocol on behalf of the routers and thereby reducing the load on the routers. To club all the issues in BGP engines at one position.

Overview:
Basically the RCP consists of three layers of components:
Top layer : Routing control server (RCS).
Middle layer : BGP engines and IGP viewers
Lower layer: routers.

The BGP engines takes care of reporting the current state to the RCS and receiving updates(routes) from the RCS which is passed on to the routers. Occasionally we get information from the Internal Gateway Protocol (IGP) viewer which gives the path cost matrix computed on the basis of OSPF or such protocols which is based on IGP link state advertisements got from routers.

This offers:
Better scalability because it manages to reduce the load on routers.
All the configuration is from the routing control server, thereby, it serves as one central point from which all the routers can be monitored or routes modification easier.
Contributes to dumbing of the router because the do very basic jobs thereby providing development independent of router software.

Basically the control program operates on the global network view and give the configuration of each device. This is also not a distributed system. This also gives a very good perspective on network effectiveness like calculation of the optimal path,etc due to its centralized system.

Current Usage:
Today AT&T uses RCP differentiating its ‘dynamic connectivity management’ offer.

Ethane

Motivation:
Enterprise networks are large and requires lots of manual configuration. Due to current systems, this results in a huge amount of down time in such networks. It also results in human errors. Further correcting is also extremely time consuming and is one of the major contributors towards IT maintenance. Currently there are middleboxes at network choke points. Problem though is that traffic could possibly be away from the middlebox location or might happen around them without the middlebox notice. More protocols are also introduced for this issue but this is not foolproof as it just adds to the complexity.

Features:
It is a new architectural model which gives a powerful model with strong security guarantees. It allows managers to define a single centralized system which enforces change at every switch very easily. It has a number of salient properties which are hard to achieve with the existing technology. The global security policy is enforced at each switch in a manner that is resistant to spoofing in Ethane. All packets can be traced to the sending host and the physical location in which the packet entered the network using the Ethane framework. Even packets processed in the past can also be tagged along the same way, a feature further added to aid in auditing. It is also provided by very simple hardware switches. This also helps in dumbing of routers and interoperability as it focusses on the reduction of the job of routers/switches.

Basic Idea:
We have already seen what circuit switching which is all fully pre established. It has been modified to go to packet switching nowadays which has its own merits and issues. Ethane combines the merits of both in a sense that it introduces a notion of a central controller which does all the complex operations like routing, naming, policy declaration and security checks.
The whole ethane framework can be broken down to the following stages:
Registration: Each user, switch and host must be registered to the controller.
Authentication: The control verifies the permissibility of a flow and all users are authenticated while the user is bound to the host in the controller.
Flow set up and forwarding: Ethane computes a route which the packet would take and adds an entry for that flow in each of the switches along the path. The switches now simply goes about forwarding them in that particular sequence.

Advantages:
This is more like a dynamic circuit switching at each flow level. The switches just check their flow table, which due to the above can be reduced to SRAMs instead of power consuming TCAMs, and forward the packets accordingly. Will help in removal of the middle boxes and some unnecessary protocols.

Probable Pitfall:
The controller needs to be extremely robust and fault resistant.