

Some Musings on OpenFlow and SDN for Enterprise Networks

David Meyer

Open Networking Summit

October 18-19, 2011

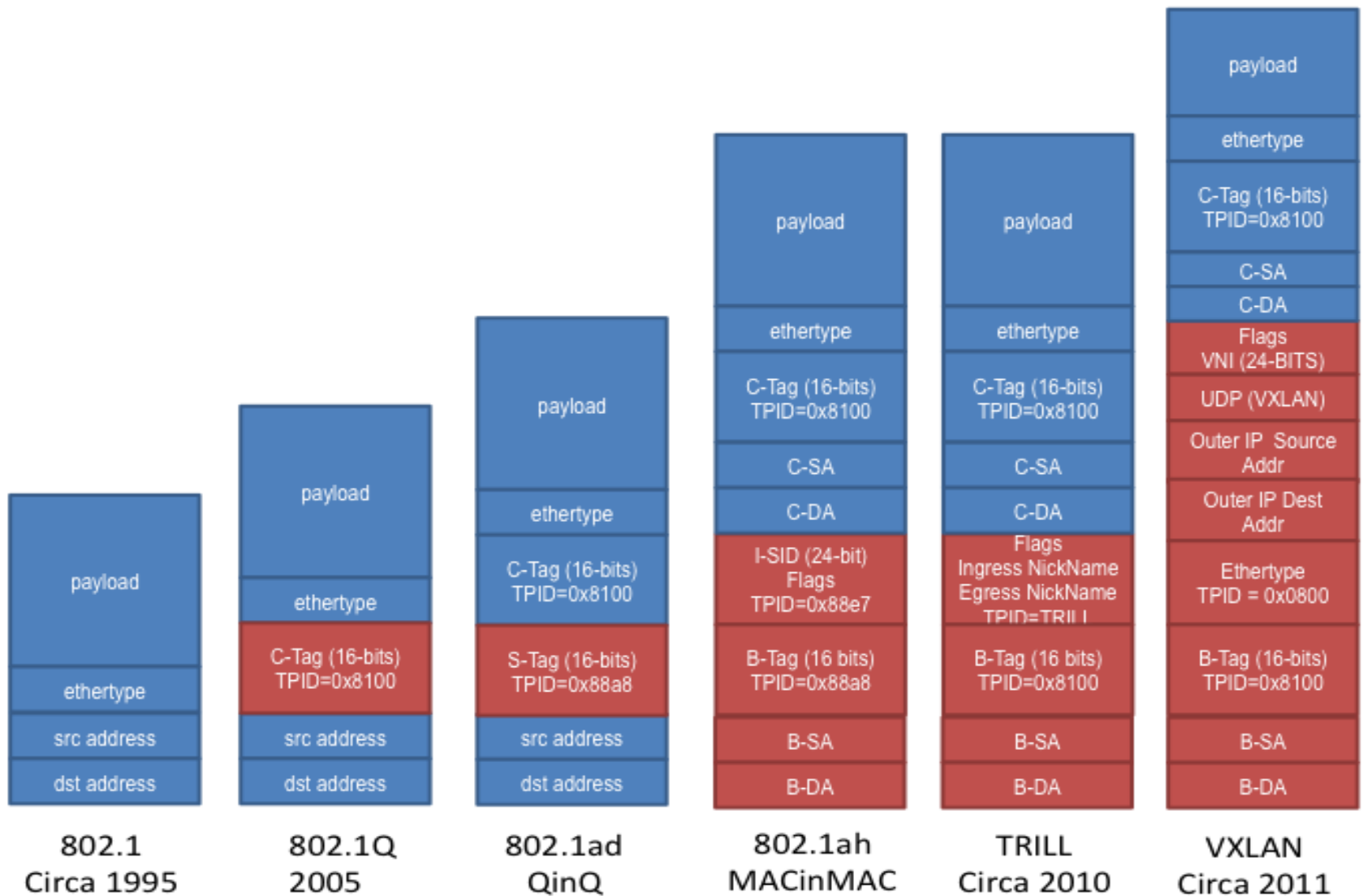
Agenda

- **Problem Space**
- **A Few Use Cases**
- **Reflections on the Promise of OF/SDN**
- **A Few Challenges and Open Questions**

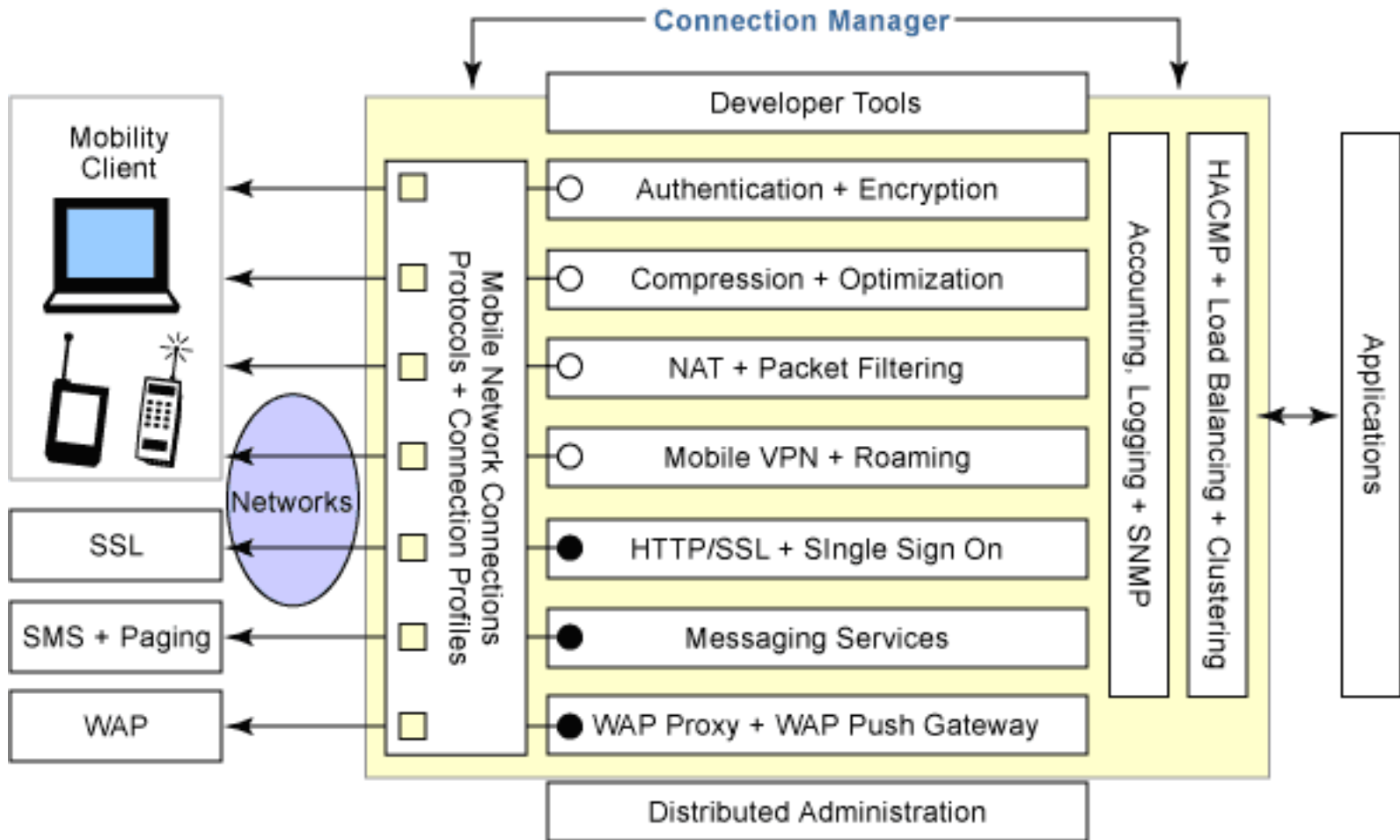
Problem Space

- Enterprise network architects and engineers are being presented with the following challenge:
 - ***Provide state of the art network infrastructure and services while minimizing TCO***
- It is the lack of ability to innovate in the underlying network results in the inability to keep pace with user requirements and to keep TCO under control
- Surprisingly general problem (or maybe not so surprising...)
 - “I have a new iPhone I want to work on the campus network...”
 - “I need my buildings to have green networking...”
 - → Constant stream of new requirements
- So what’s the problem?

At Least Ethernet is still simple...



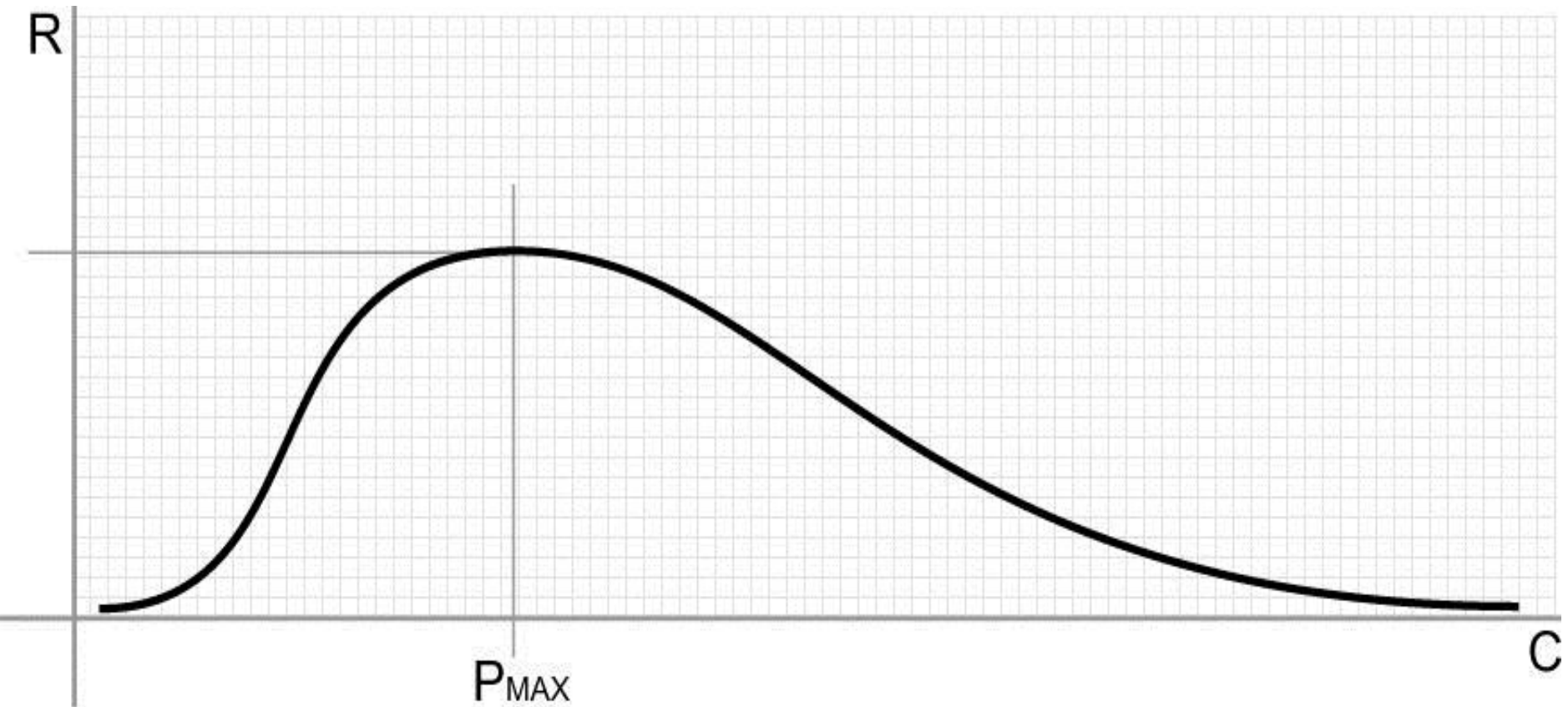
Basically, protocol soup...



Many protocols, many touch points, few open interfaces or abstractions, ... →

Robustness vs. Complexity

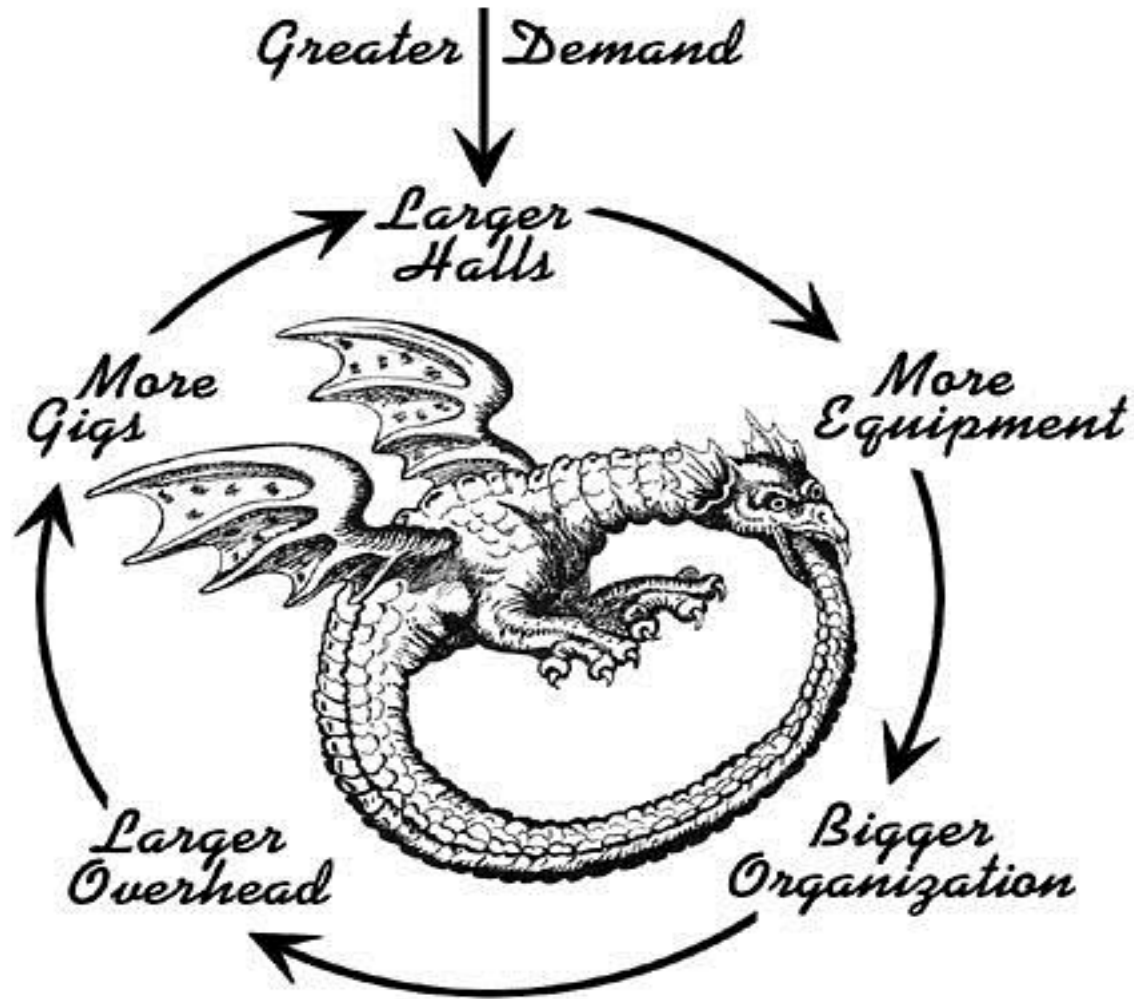
“Systems” View



Increasing number of protocols, configurations and interactions



Complexity/Robustness Spirals



See J. Doyle, et. al., "Robustness and the Internet: Theoretical Foundations"

What Tools Does OF/SDN Give Us Address This Growing Complexity?

- **Forwarding abstraction**
 - OpenFlow/Flow Space
- **Distributed State Abstraction**
 - Global Network View (Logical and Virtual)
- **Distributed Network Control Abstraction**
 - Network Operating System (NOS)

These Abstractions Give Us...

- **A unified way of thinking about network “boxes”**
 - Routers, Switches, Firewalls, NATs, Load Balancers,...
- **A centralized view of the network**
 - Simplified control logic/operations
- **Mechanisms for decoupling policy from configuration**
 - OF/SDN doesn't do this directly, but rather makes such decoupling possible

A Few Enterprise Use Cases

- **Dynamic Network Access Control**
 - I'll say more about this in a minute
- **Load Balancing**
 - Network
 - Server
 - Latency Equalized Routing
- **Distributed Firewalls and NATs**
- **Network Virtualization**
 - Enterprise Cloud (XaaS)
 - VM Migration and User Mobility
 - Virtual Edge Provisioning
 - “Slicing”
- **Energy-Efficient/Proportional Networking**
- **Adaptive Network Monitoring**

So What is The Promise of OF/SDN?

- Consider “Decoupling Policy from Configuration in Campus and Enterprise Networks” by Nick Feamster and colleagues at GA Tech:
 - <http://www.gtnoise.net/papers/2010/feamster:lanman2010.pdf>
- The study shows how the unified view of network devices coupled with a global network view provided by OF/SDN allows an elegant decoupling of policy and configuration in the context of wireless LAN access control

Typical Registration on a Wireless LAN

During registration, **systems are scanned** for known vulnerabilities. If the scan reveals vulnerabilities, the user is presented with these vulnerabilities and given an opportunity to **update the system**. The **firewall** for the network allows traffic to get to the appropriate update servers for Microsoft and Apple. The **registration VLAN** uses a firewall to block network traffic to unregistered desktops. However, **the firewall allows Web and secure Web** (i.e., port 80 and 443) traffic to pass so that desktop machines can reach update sites. **Various routers and switches are employed to facilitate creating the VLANs necessary for the needed networks**. The local switches determine which VLAN for each machine that joins the network. The **switch will download VLAN maps** periodically from a VMPS. **Unknown MAC addresses are assigned to the unregistered VLAN and known MAC addresses are placed onto the appropriate subnet**. VMPS periodically downloads the VLAN maps from the registration server. **Network security is enforced by creating ARP tables that map each MAC address to its registered IP and pushing that table to each router**.

Rather...Define State Transitions for a Host

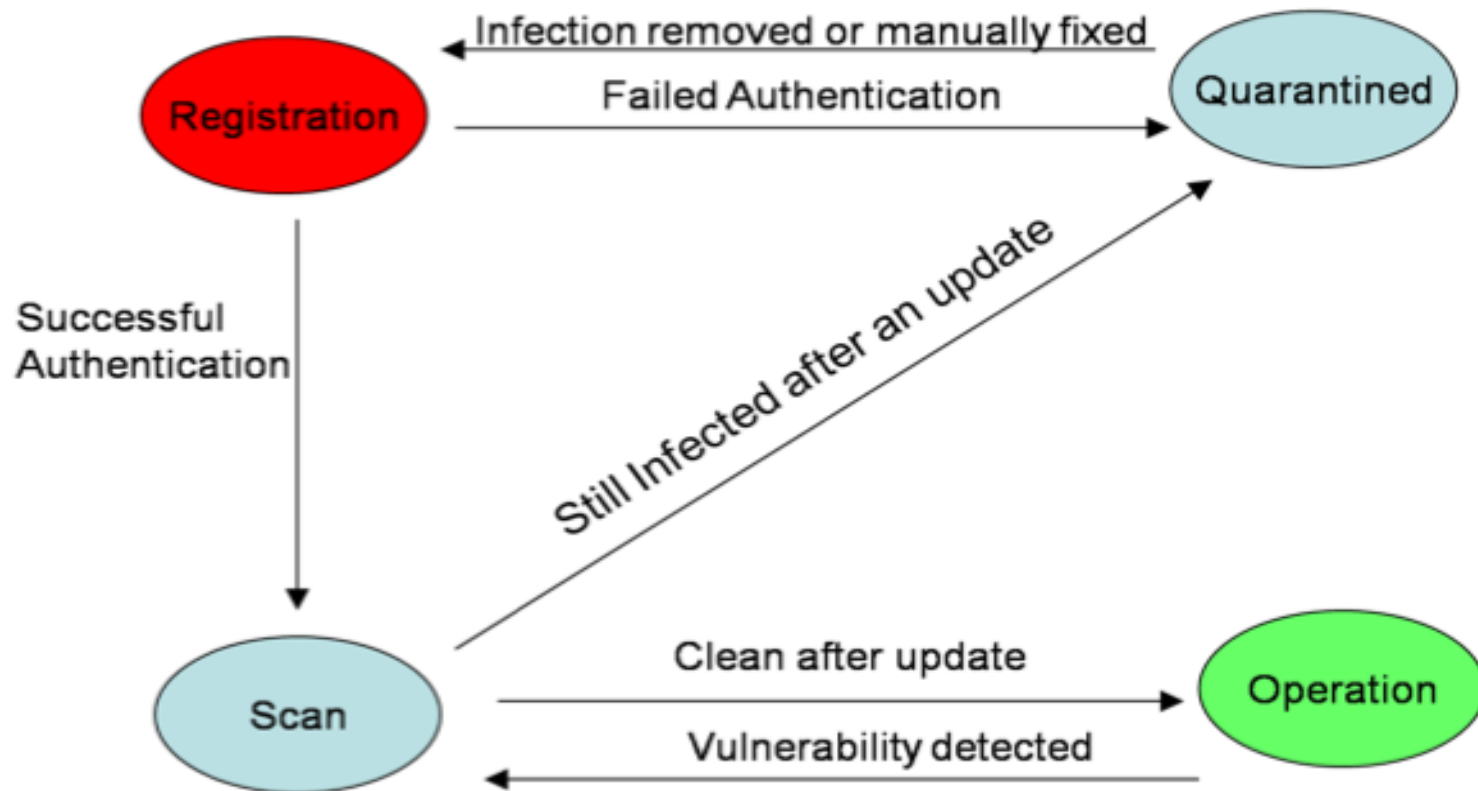


Fig. 2. State transitions for a host. The controller tracks the state of each host and updates the current state according to inputs from external sources (e.g., network monitors).

Decoupling Policy and Configuration

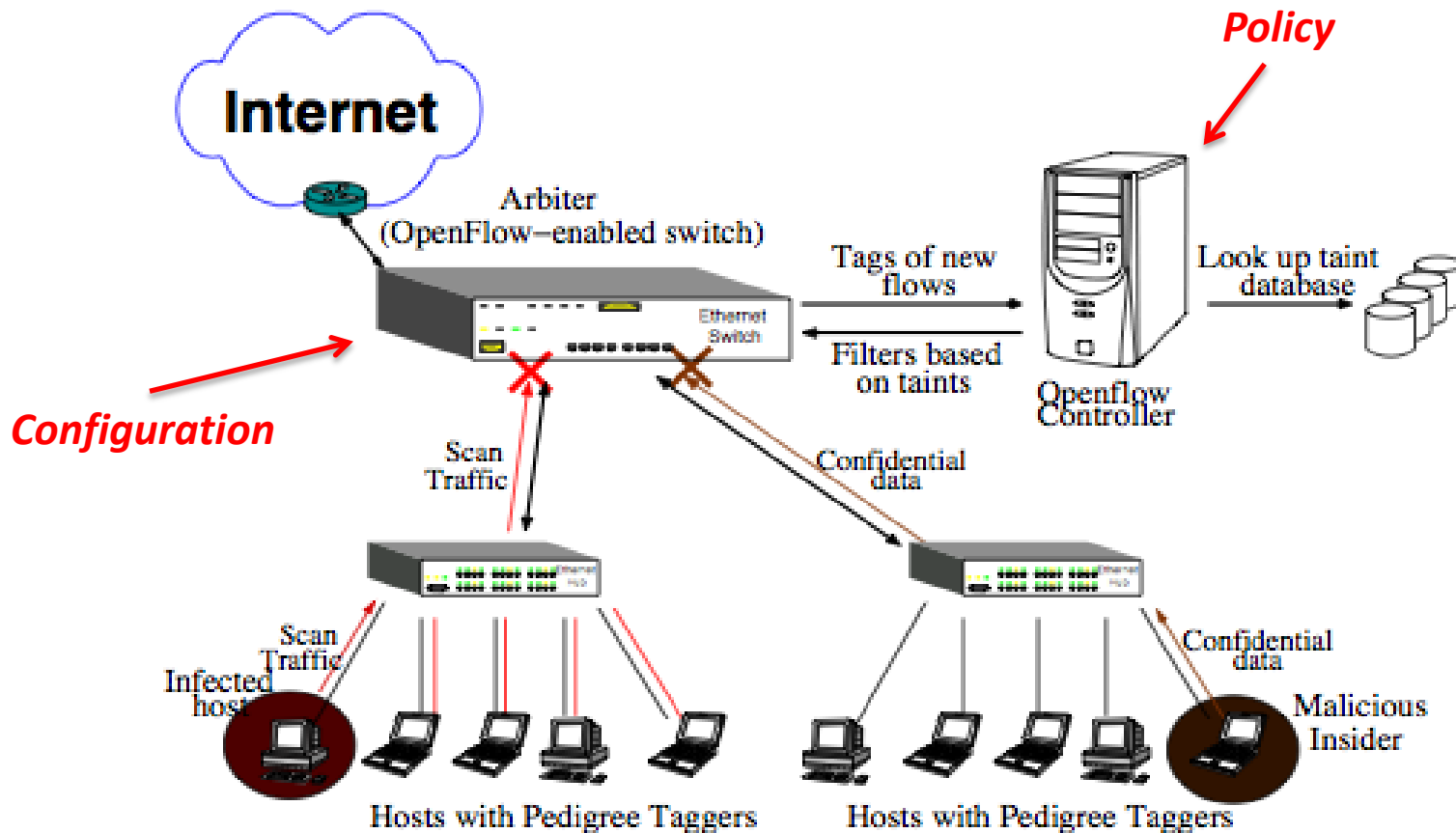


Fig. 5. Pedigree deployment in an enterprise network, where a malicious host is trying to scan its local network.

A Few Challenges/Open Questions

- **Theoretical/Scientific Foundations for SDN**
 - A new way of thinking about networking with a wide variety of intellectual challenges
 - Distributed systems, theory, network architectures, programming languages, ...
- **Stabilize/Extend the OpenFlow Protocol**
 - Work well underway in the ONF
- **Programming Languages/Models/Systems**
 - Composition of applications
 - Part of the goal of Frenetic
 - Generic ways to handle streams
 - Functional Reactive Programming promising (e.g. Nettle)
 - Tool chains
- **Hybrid Switch Model**
 - Interaction between on-board control planes and external control planes
- **NOS/Network Hypervisor Scalability**
 - Proactive vs. reactive flow instantiation
 - Transactional throughput
 - Distributed/replicated controller infrastructure
 - Switch Heterogeneity
- **Operational Practices and Tools**

Thanks!