High-speed Networks, Cybersecurity, and Software-defined Networking Workshop

Jorge Crichigno
University of South Carolina

Western Academy Support and Training Center (WASTC)
2020 Summer Conference
June 15 -19, 2020

National Science Foundation (NSF), Office of Advanced Cyberinfrastructure (OAC) and Advanced Technological Education (ATE)

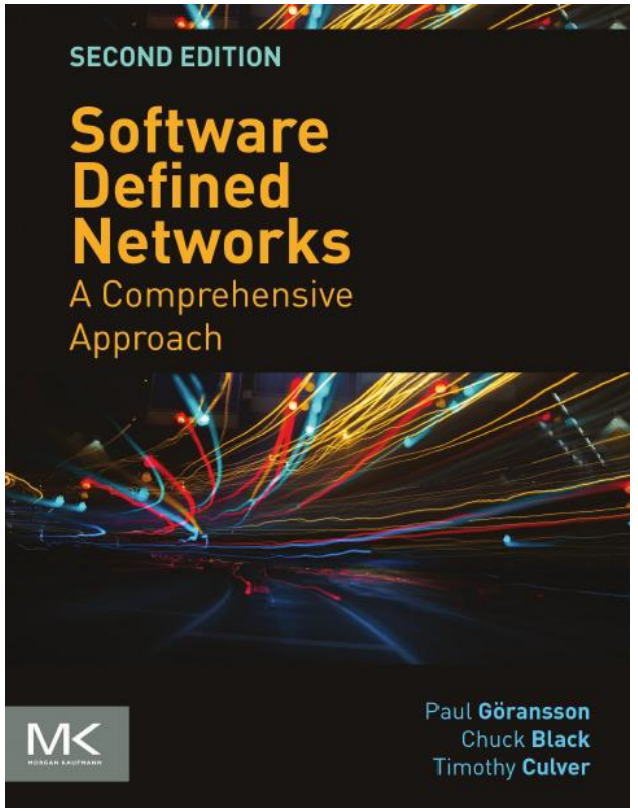
Chapter 1: Introduction

Software Defined Networks (SDN)

- What is the SDN?
- Much information is available about SDN
  - Papers
  - Videos
  - Books
- However, there is no systematic lab series for IT students and practitioners
  - Background overview
  - Companion labs

Software Defined Networks (SDN)

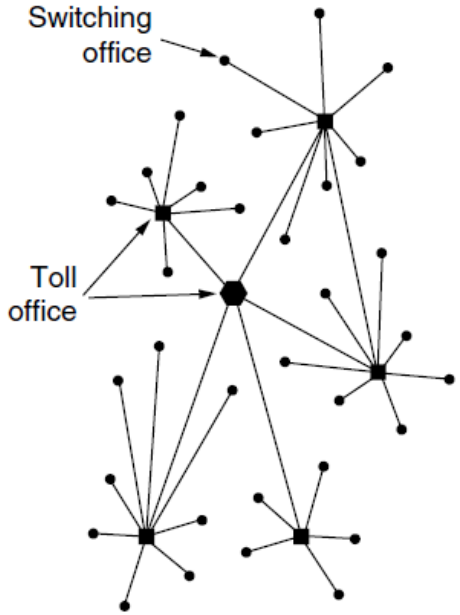
- The goal of the SDN Lab Series is to provide a practical experience to students and IT practitioners
- The labs provide background information which is reinforced with hands-on activities
  - A good book on SDN network (which matches the SDN Lab Series) is “Software Defined Networking, A Comprehensive Approach”
  - The book is also very approachable for undergraduate and graduate students, networking professionals, and IT managers



Section 1.2: Historical Background

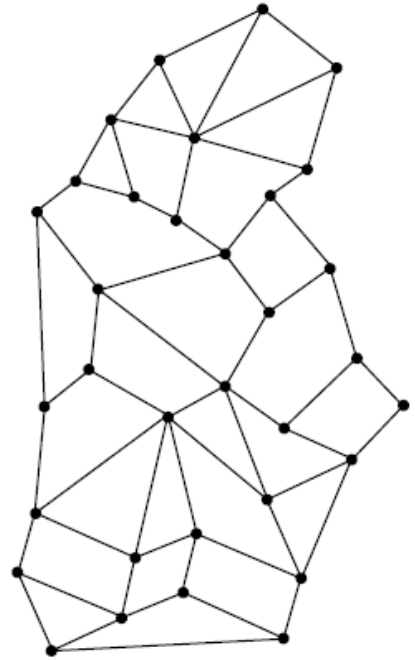
Historical Background

- The major communications networks around the world in the first half of the 20th century were the telephone networks
  - Composed of switching offices, each of which was connected to thousands of telephones
  - Switching offices were, in turn, connected to higher-level switching offices (toll offices), to form a national hierarchy
  - The vulnerability of the system was that the destruction of a few key toll offices could fragment it into many isolated islands



Historical Background

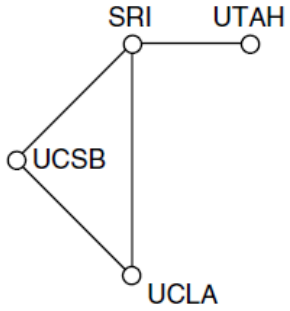
- Paul Baran, a Polish immigrant who became a researcher working at Rand Corporation in the US around 1960, argued that in the event of enemy attack networks like the telephone network were easy to disrupt
- Mr. Baran's proposed solution was to transmit the voice signals of the phone conversations in packets of data that could travel autonomously – survivable networks (1964)[1]
  - Digital packet-switching technology



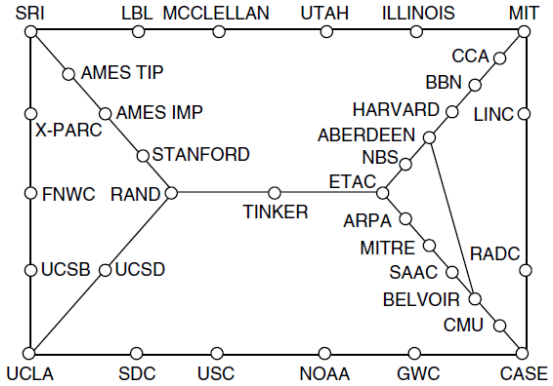
1. P. Baran, Baran, Paul, "On Distributed Communications: I. Introduction to Distributed Communications Networks," RAND Corporation, 1964. https://www.rand.org/pubs/research_memoranda/RM3420.html

Legacy Networks Overview

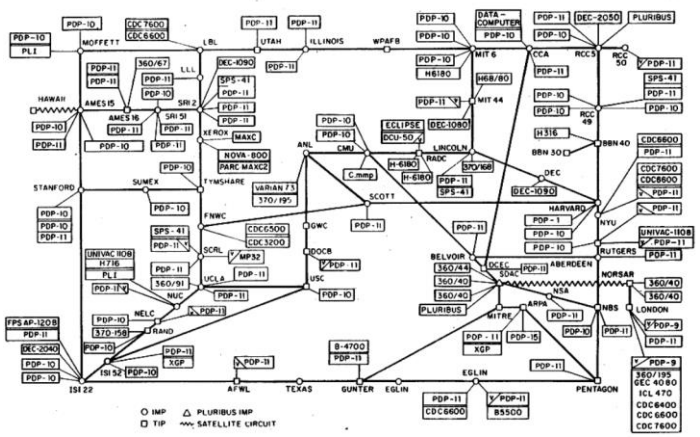
- A network called ARPANET eventually was implemented using Baran's ideas
  - Funded by the U.S. Advanced Research Projects Agency (ARPA)
- This *decentralized*, connectionless network grew over the years until bursting upon the commercial landscape around 1990 in the form of the Internet
- The Internet was a distributed, connectionless architecture



1969



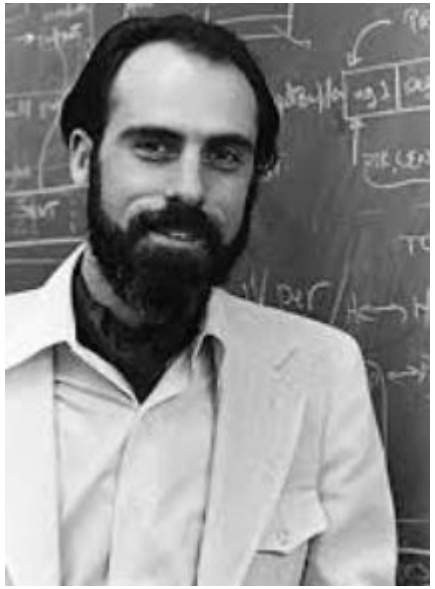
1972



1977

Legacy Networks Overview

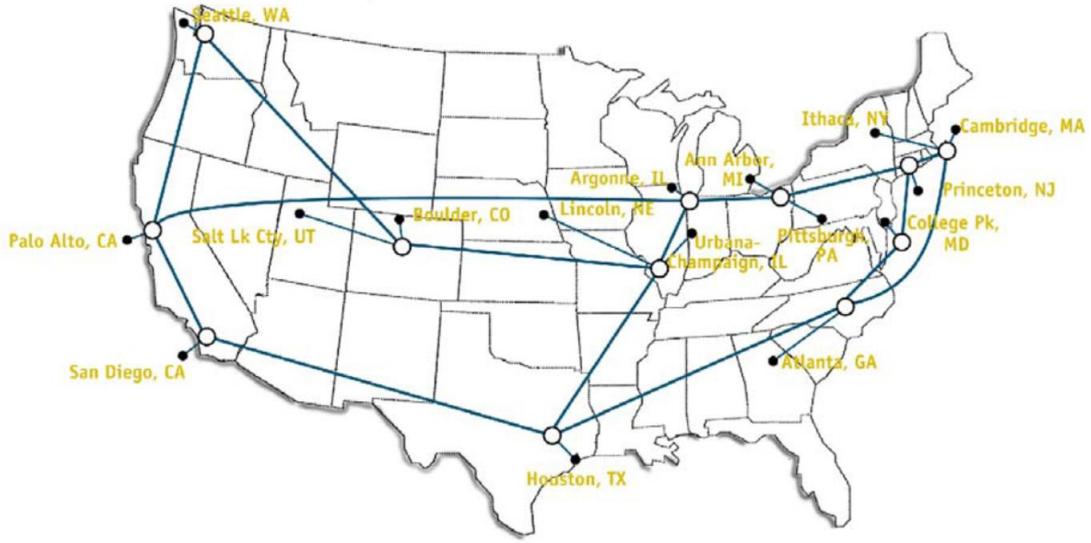
- In the early days, existing protocols were not suitable for running over different networks
- In 1974, TCP/IP model and protocols were invented by Robert Khan and Vinton Cerf[1]



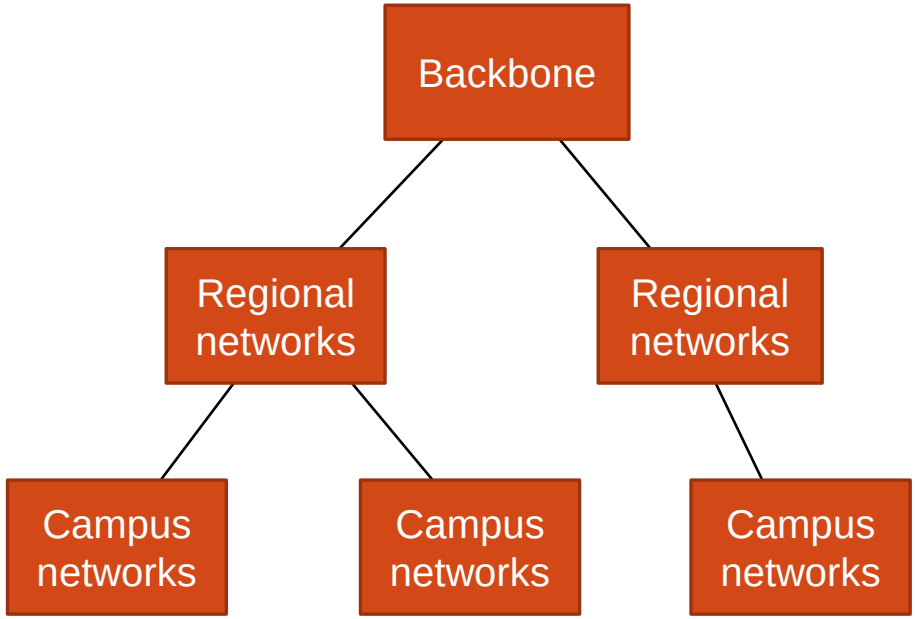
1. V. Cerf, R. Kahn, “A Protocol for Packet Network Intercommunication,” IEEE Trans. on Comms, vol. 22, No 5, 1974.

CSNET and NSFNET

- In 1981, the National Science Foundation (NSF) established the Computer Science Network (CSNET) to provide connect (to ARPANET and other networks) to all university computer scientists
- In 1985, NSF established the NSFnet to link together five supercomputer centers that were then deployed across the U.S.



NSFNET backbone



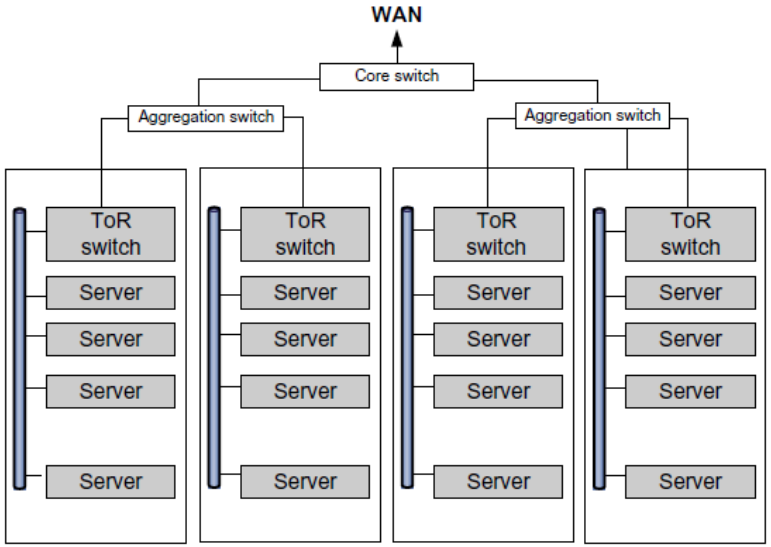
Section 1.3: The Modern Data Center

The Modern Data Center

- In 1991, NSFNET lifted its restrictions on the use of NSFNET for commercial purposes
- NSFNET itself would be decommissioned in 1995, with Internet backbone traffic being carried by commercial Internet Service Providers (ISPs)
- The main event of the 1990s was to be the emergence of the World Wide Web
  - Invented at CERN by Tim Berners-Lee between 1989 and 1991
- The web brought the Internet into the homes, businesses, millions of people

The Modern Data Center

- A number of companies emerged as big winners in the Internet space
  - Microsoft, Cisco, Yahoo, e-Bay, Google, Amazon
- The web gave rise to data centers, hosting heavily subscribed web services
- Servers were physically arranged into highly organized rows of racks of servers
- Racks were hierarchically organized such that Top-of-Rack (ToR) switches provided the networking within the rack and the inter-rack interface capability



The Modern Data Center

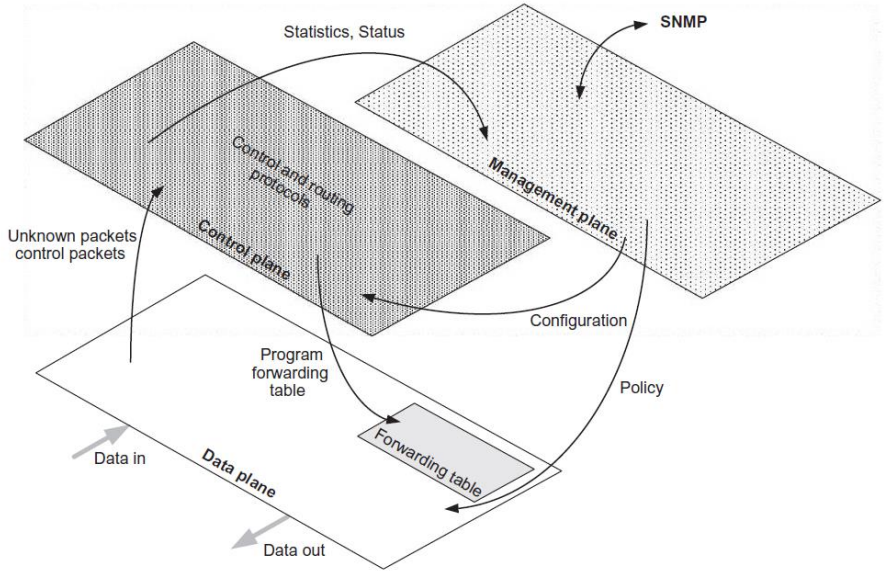
- A modern physical servers can host hundreds of virtual machines (VMs), results in thousands (or even millions) of VMs communicating within the datacenter
- These VMs are now communicating via a set of protocols and devices that were optimized to work over a large, disparate geographical area with unreliable links
- While still important, survivability was not that relevant (in contrast to 1970s, 1980s WANs) in the emerging data center
- Network management systems designed for carrier public networks or large corporate intranets simply cannot scale to these numbers
- A new network management paradigm was needed

While the modern data center was the premier driver behind the SDN fervor, by no means is SDN only applicable to the data center

Section 1.4: Traditional Switch Architecture

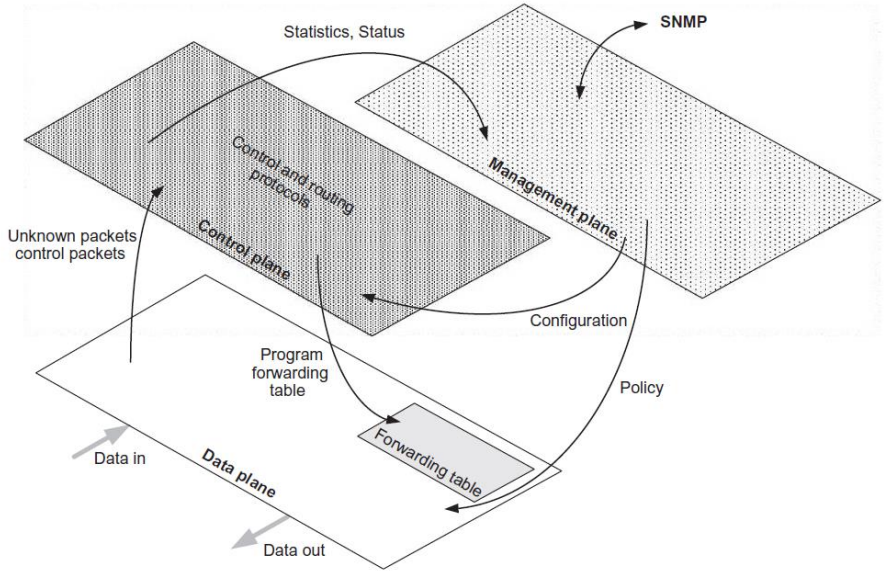
Data, Control, and Management Planes

- The data plane consists of the various ports that are used for the reception and transmission of packets and a forwarding table with its associated logic
- The data plane assumes responsibility for packet buffering, packet scheduling, header modification, and forwarding
- If an arriving packet's header information is found in the forwarding table, it may be forwarded without any intervention of the other two planes



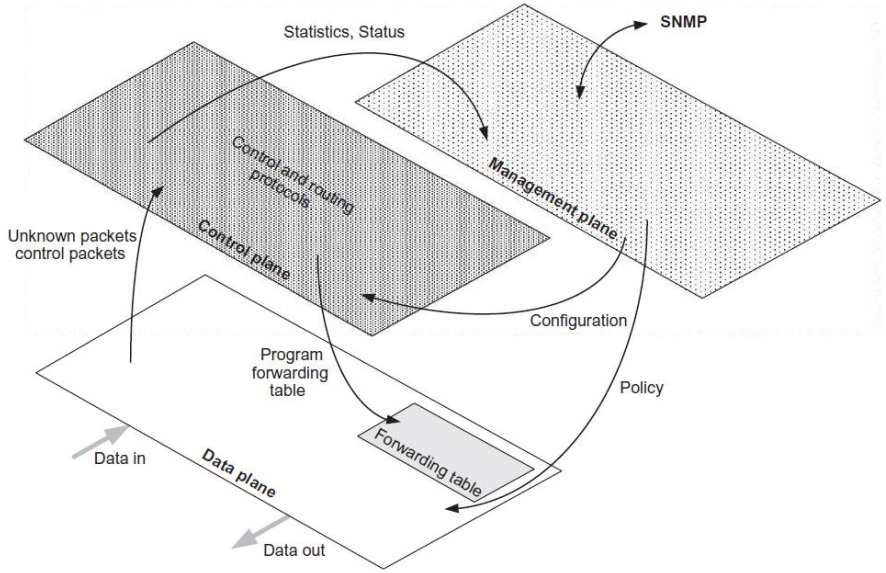
Data, Control, and Management Planes

- Not all packets can be handled exclusively at the data plane, sometimes simply because their information is not yet entered into the table, or because they belong to a control protocol that must be processed by the control plane
- The main role of the control plane is to keep current the information in the forwarding table so that the data plane can independently handle as many packets as possible



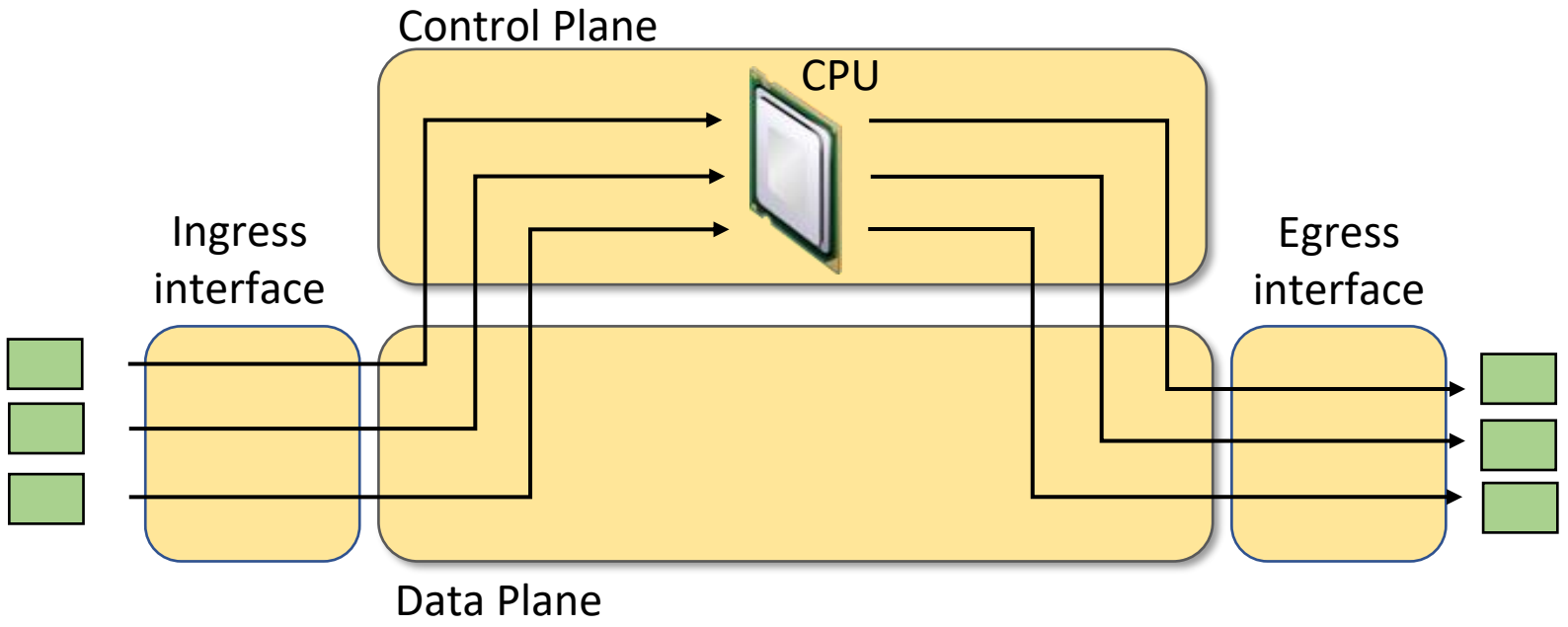
Data, Control, and Management Planes

- Network administrators configure and monitor the switch through the management plane
- The management plane extracts information from or modifies data in the control and data planes as appropriate
- The network administrators use some form of network management system to communicate with the management plane in a switch (e.g., command-line interface)



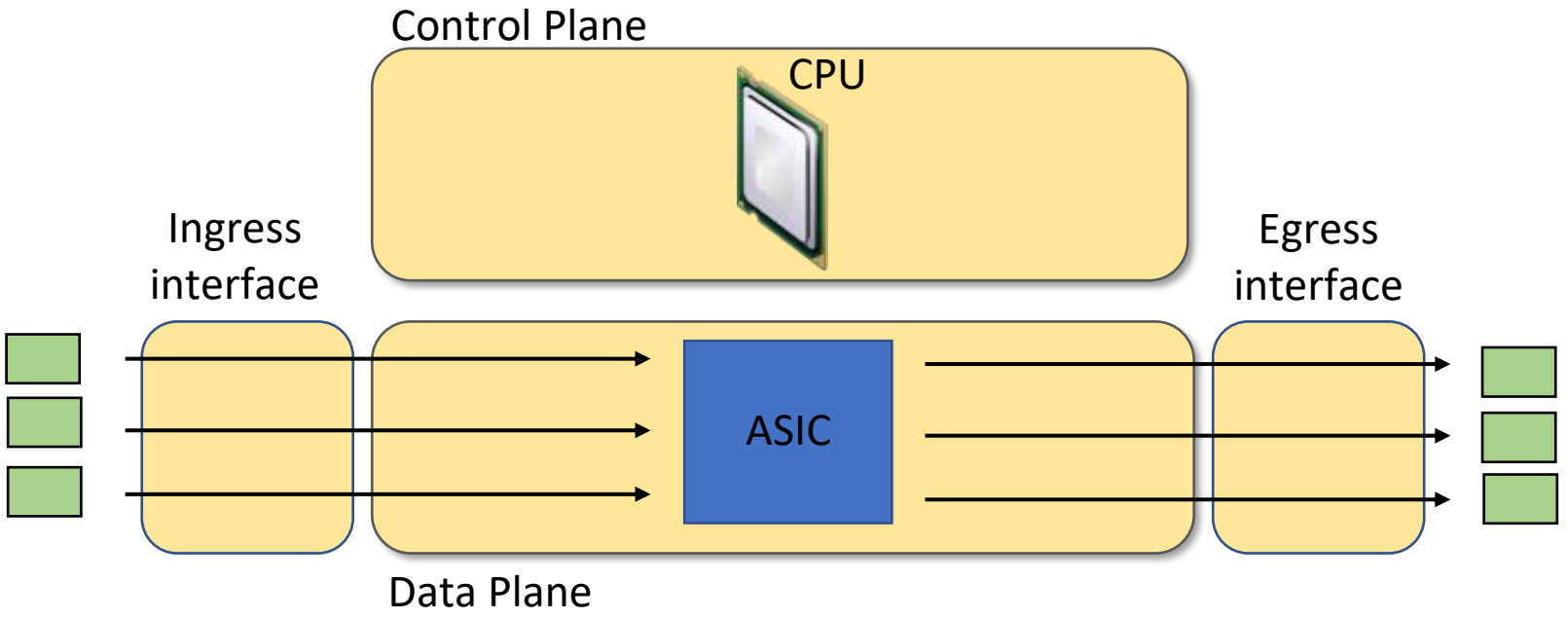
Software-based Routing and Bridging

- When a packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table
- The router does this for every packet



Hardware Look-up of Forwarding Tables

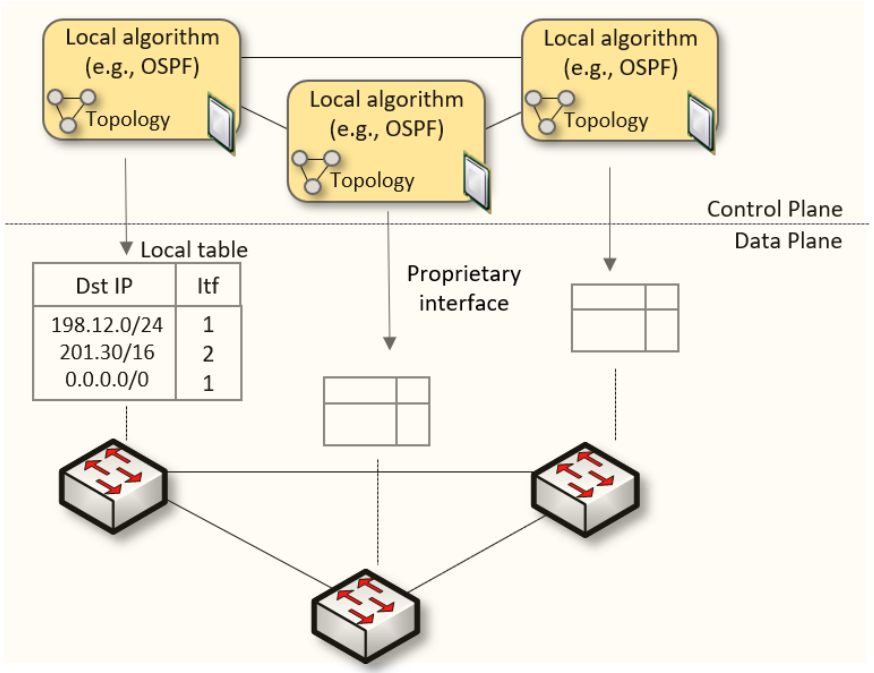
- The first major use of hardware acceleration in packet switching was via the use of Application-Specific Integrated Circuits (ASICs) for table look-ups
- In the mid-1990s advances in Content-Addressable Memory (CAM) technology made it possible to perform very high speed look-up using destination address fields



Section 1.5: Autonomous and Dynamic Forwarding Tables

Autonomous and Dynamic Forwarding Tables

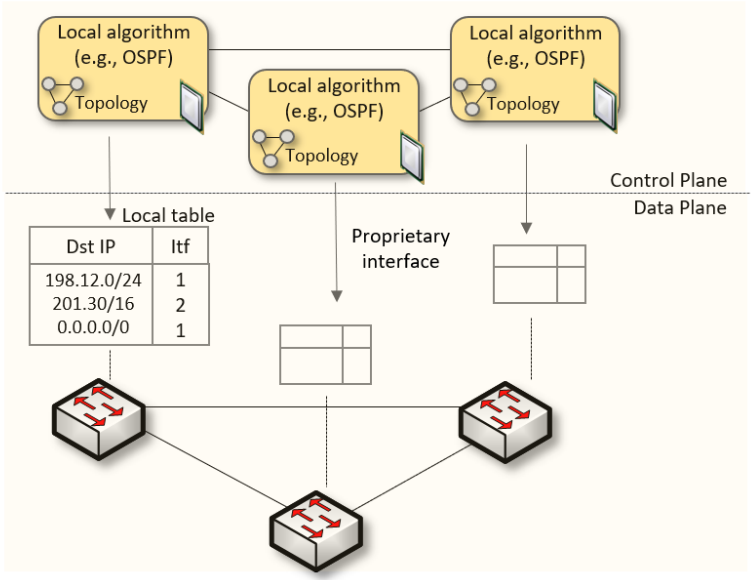
- The interface between the control plane and data plane has been historically proprietary
- A router was a monolithic unit built and internally accessed by the manufacturer only
  - Vendor dependence; slow product cycles of vendor equipment, standardization



Autonomous and Dynamic Forwarding Tables

- Traditional routers run algorithms to determine how to program its forwarding table

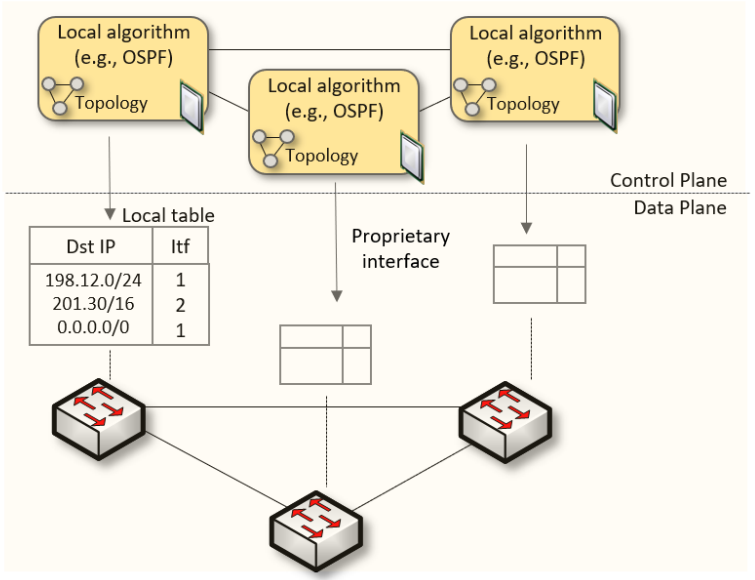
Legacy network



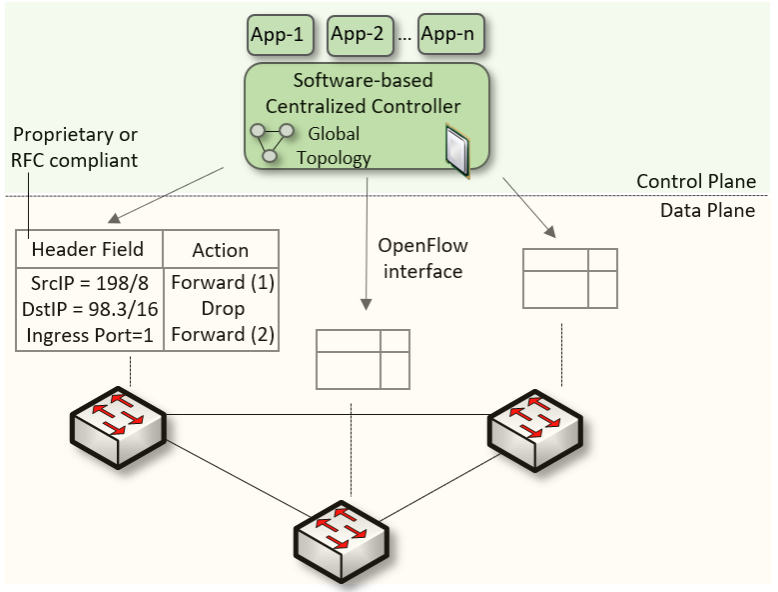
Autonomous and Dynamic Forwarding Tables

- Traditional routers run algorithms to determine how to program its forwarding table
- In SDN networks, that function is now performed by the controller
  - The controller is responsible for programming packet-matching and forwarding rules

Legacy network



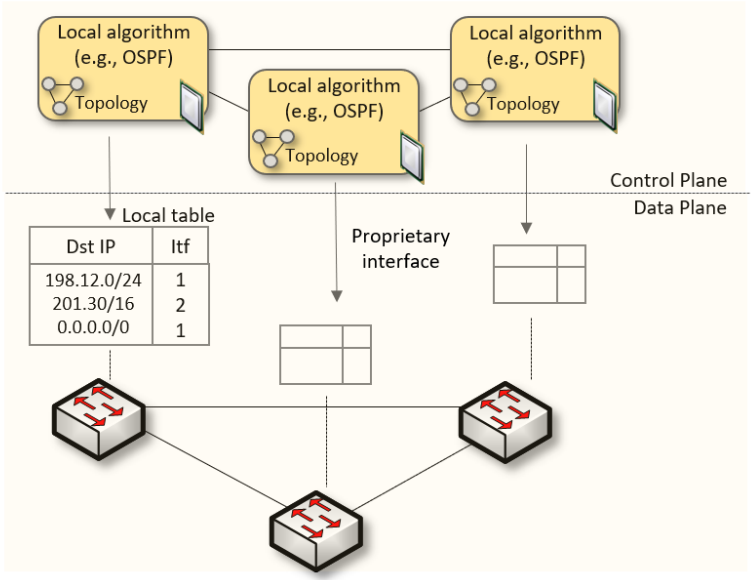
SDN network



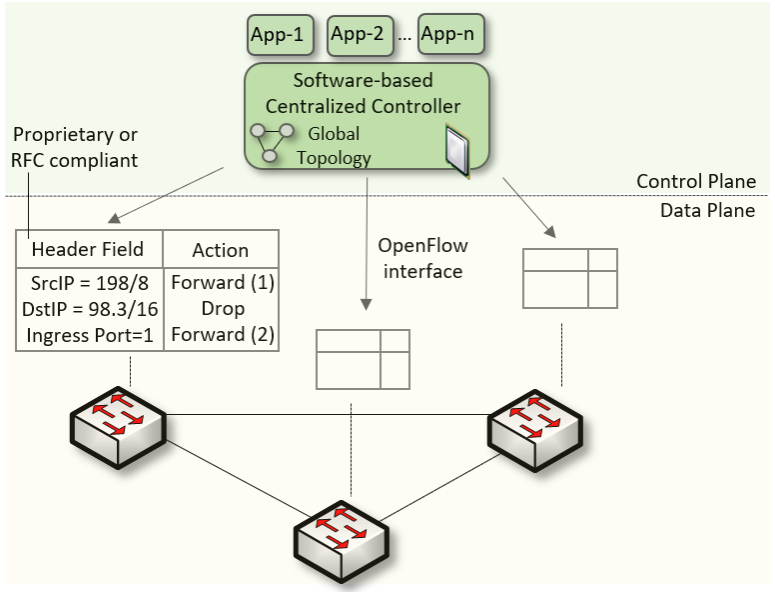
Advantages of SDN Networks

- Ease of network management
- Enforcement of security policies
- Customized network behavior
- Possibility of experimentation and innovation (custom policies, apps can be deployed)
- Packets can be forwarded based on other fields, such as TCP port number

Legacy network



SDN network

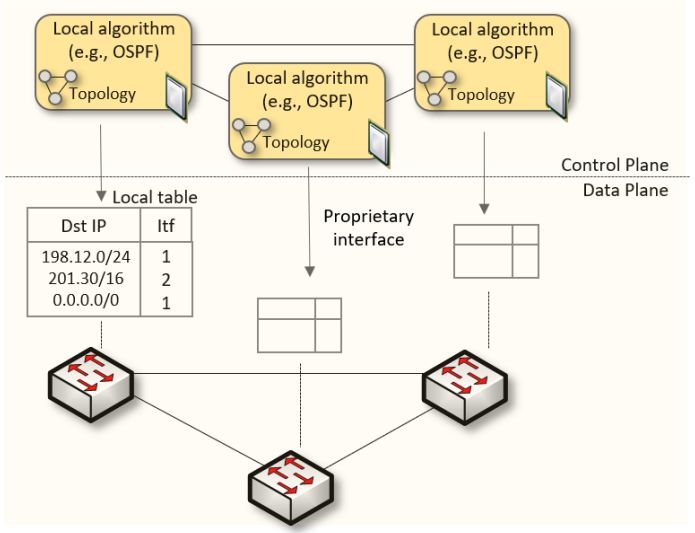


Section 1.7: Open Source and Technological Shifts

Open Source and Technological Shifts

- The open source model has revolutionized the way software is developed / delivered
- Functionality that used to be reinvented in every organization is now readily available
  - Linux, OpenSSL, open-source routing protocol stacks (BGP, OSPF, RIP, etc.)
- More SDN enabled switches (Cisco, Juniper, etc.), white box programmable switches (Edgecore, Stordis), SDN applications
- Increase of the the pace of innovation, fostered by the agility of software development

Legacy network



SDN network