Networking 101

The basics

Bio

David Forrest graduated from Oregon State University in BA, Finance Emphasis, Physics & Mathematics. Lifelong hobbyist in IT from IBM 1401, Model 20, Model 30, Model 85, Sigma 7, XDS 7, SWTP 6800, M6809, 8080, 80286, 80386, OS2, and on to currently running XP, CentOS6/7, Raspbian, Mint, and Chrome on various local and cloud machines.

A presentation pdf available at:

http://maplepark.com/~drf/RemoteReads/20181212_Networking_101

Computer Networks

Everything is Connected

- Internet
- Cell Phones
- Wireless Laptops
- Wired Homes
- Refrigerators
- Toasters
- Security Cameras

Industry Standards vs Vendor Standards

Standards are great like the standard measure of weight or distance. They help people communicate facts about the size and weight of things. Even Time measurement has various standards. In the technology industry some standards are driven by organizations of volunteers and some by vendors pushing an agenda. In computer networking standards also need to have a use base and adoption to be useful to the end user.

Complexity in Computer Networking

Just like Big and Little Endian there are a swath of simple concepts wrapped up to form modern computer networking communication. Various protocols and standards exist to enable us to communicate better. Standards like IPv4 exist so that two or more systems can communicate efficiently. The protocols are layered in such a way that it again can become difficult to communicate a standard. So some terms like TCP/IP have come about which poorly identify a “stack”. Historically organizations have had disparate stacks which made interoperability difficult.

Computer Network Today

Being all about the consumer today’s computer networks are dynamic. They announce the protocols and standards used to communicate with each other. Modern things like DHCP enable the systems to get connected faster.

Protocols and Layers

Protocols

“In telecommunications, a communication protocol is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, **or a combination of both**.”

https://en.wikipedia.org/wiki/Communications_protocol

Layers

“In computing, an abstraction layer or abstraction level is a way of hiding the implementation details of a particular set of functionality, allowing the separation of concerns to facilitate interoperability and platform independence.” https://en.wikipedia.org/wiki/Abstraction_layer

As we will discuss the historical standards differ from today’s network reality. It is important to understand that at times software like the Linux Kernel is too awesome and enables you to create infinite layers of abstraction, namespaces and yes, even Computer Networks!

OSI Model Layers (Software)

“The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defines seven layers.”

https://en.wikipedia.org/wiki/OSI_model

** Outdated over the last two decades with the adoption of Software Defined Networking (SDN)

Physical Networking

Physical Transport

At the base of all modern communication are technologies like Frame Relay and Time Division Multiplexing (TDM) which are built to manage digital signals over a physical medium. There are a confusing array of standards and protocols at the physical layer. Consider this the layer that you can feel the buzz of electricity from if you are numb to it.

Physical layers over Electrical Conductor, Fiber Optics, and Wireless MODEM are the most common with Quantum Entanglement being outside the scope of this talk.

Message Transmission Unit (MTU) (Ethernet)

The physical transfer of data is commonly unitized into packets of fixed size to allow verification of accurate receipt. The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

Ethernet frames of data can be conceived as similar, requiring a series of verified packets to make up the frame. The IPv4 protocol commonly uses 1500 8-bit bytes as the MTU while IPv6 uses 1280-1500 bytes.

ISP to a Home

Most homes have a Customer Premise Router (CPE) which uses a modulator-demodulator (Modem) to communicate with an Internet Service Provider (ISP) over a protocol like Data Over Cable Service Interface Specification (DOCSIS) or Digital subscriber line (DSL) and optionally on modern networks Ethernet. The connection from the ISP to the CPE in the home is one network. To communicate over that network there are routers on each side of the network. The router might do things like adjust the data packet size to work over the network or queue the packets for transmission.

Internet vs Intranet

Inside your home premise you may have an Intranet where the network is internal to your home and the connection via router to the Internet which is outside your home. These are two networks that are connected via a router to enable you to look at pictures of cats. Huge amounts of work have gone into making cat (and dog) photos accessible by consumers.

Larger premises may have disparate interests such as campuses, departments, or entities just related by the fact that a virtual interface has been created.

Software Defined Networking

Layers on Layers on Layers

Software-defined networking (SDN) technology is an approach to computer networking that allows network administrators to programmatically initialize, control, change, and manage network behavior dynamically via **open interfaces** and provide abstraction of lower-level functionality. SDN is meant to address the fact that the static architecture of traditional networks doesn't support the dynamic, scalable computing and storage needs of more modern computing environments such as data centers. This is done by decoupling or disassociating the system that makes decisions about where traffic is sent (the SDN controller, or control plane) from the underlying systems that forward traffic to the selected destination (the data plane).

Architecture

Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today’s applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow® protocol is a foundational element for building SDN solutions.

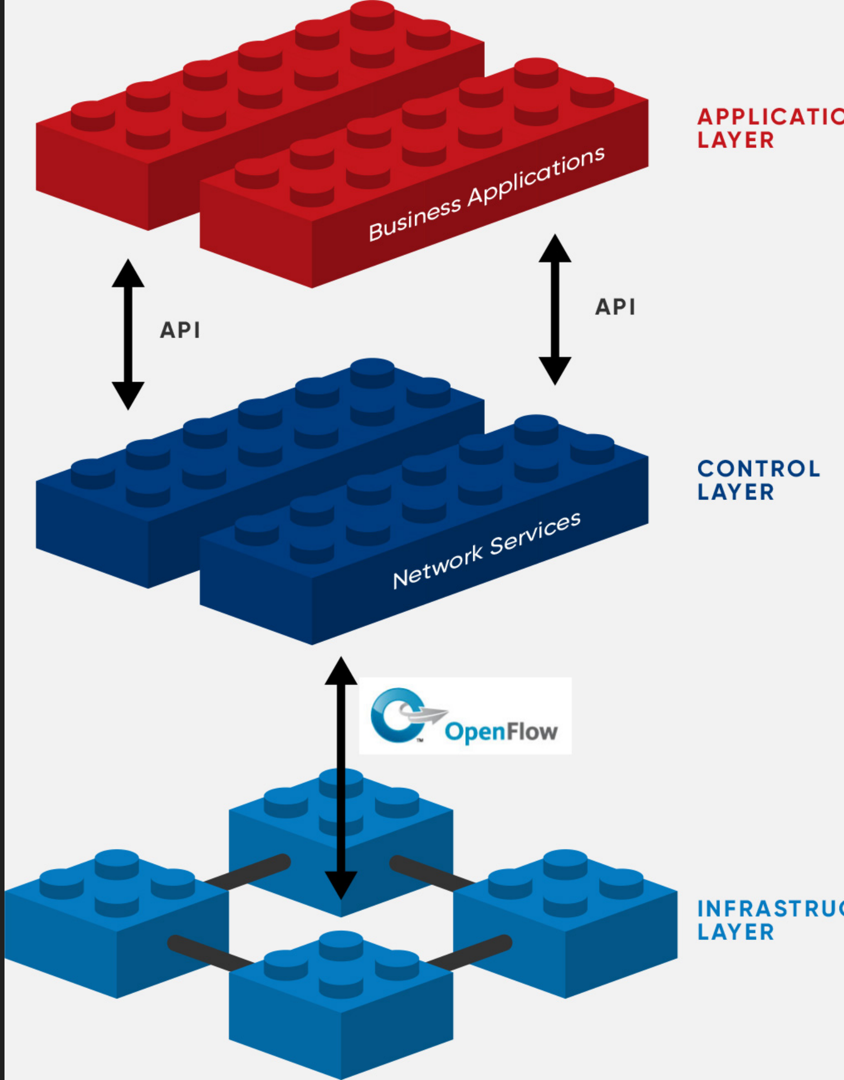
Open Networking Foundation (ONF) is a non-profit operator led consortium

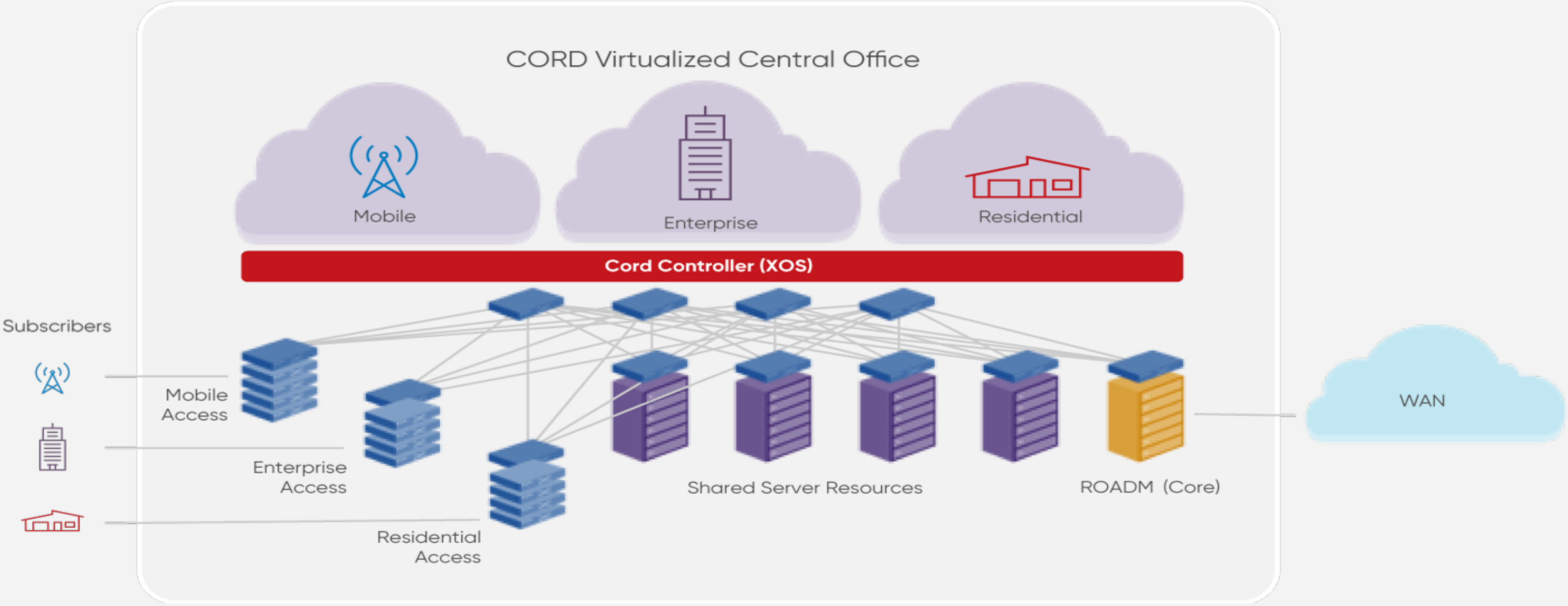
DIRECTLY PROGRAMMABLE

Network control is directly programmable because it is decoupled from forwarding functions.

AGILE

Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.




CORD Virtualized Central Office
Mobile
Enterprise
Residential
Cord Controller (XOS)
Subscribers
Mobile Access
Enterprise Access
Residential Access
Shared Server Resources
ROADM (Core)
WAN

VLANs, MPLS, and Bridges

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. https://en.wikipedia.org/wiki/Virtual_LAN

Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks. https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. https://en.wikipedia.org/wiki/Bridging_(networking)

Namespacing or Named Layers

Most of the protocols and methods create namespaced layers on the basic network transport protocols to isolate themselves. VLANs, MPLS, and Bridges are just like the stacking doll toys, they create new layers and enable you to create complexity without additional physical equipment. You can put VLANs inside a VLAN and run a MPLS network on top of another MPLS network. Bridging is one of the more common tools that modern Linux systems will use to isolate networks. Modern containerization tools like Docker create an isolated bridge network so they can control access to the containers for security.

Simple Linux Bridge

```
ip link set dev enp0s25 up

ip link set dev fakenet up

brctl addbr mybridge
```

My focus/interest here

I have purchased a gigabit PC-Engines apu2 platform which I intend to work on as a lab router to distribute container sharing at the network level to cloud machines in the Dallas and New York area. This arena of multicasting bridged interfaces was covered in a presentation to the St. Louis Unix Users Group on March 8, 2017

http://maplepark.com/~drf/RemoteReads/20170308_IPv6Multicast.pdf

And I wanted to explore further …

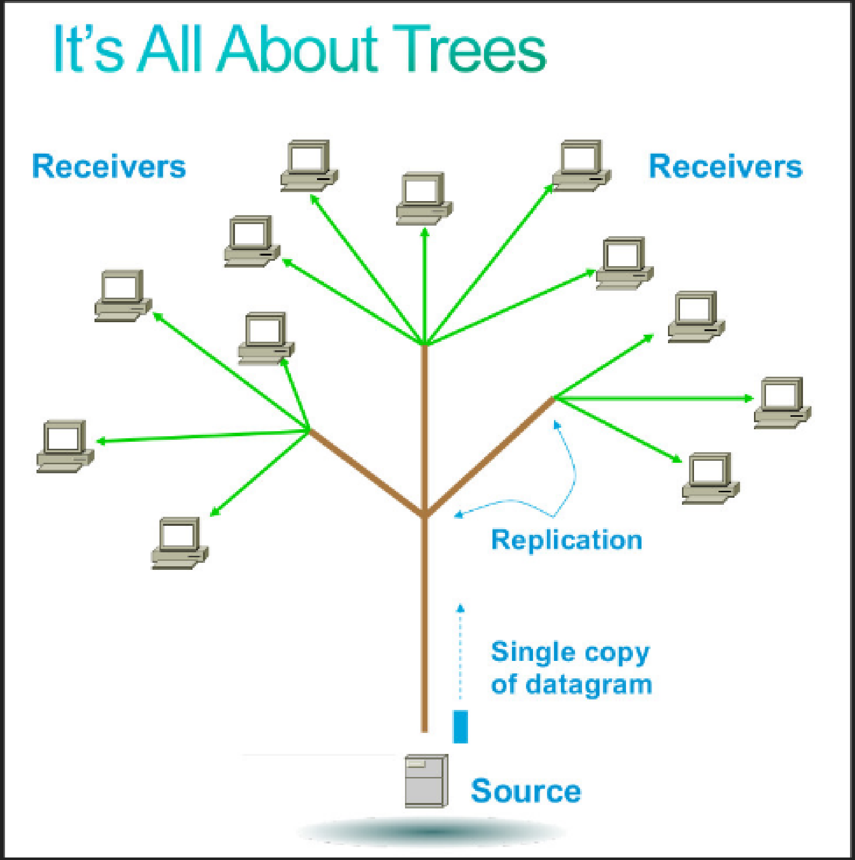
But NATing is not an option for me!

In IPv4 it is very difficult for an organization to get even one globally routable multicast group assignment, and the implementation of inter-domain solutions is arcane. Unicast address assignments by a local Internet registry for IPv6 have at least a 64-bit routing prefix, yielding the smallest subnet size available in IPv6 (also 64 bits). With such an assignment it is possible to embed the unicast address prefix into the IPv6 multicast address format, while still providing a 32-bit block, the least significant bits of the address, or approximately 4.2 billion multicast group identifiers. Thus each user of an IPv6 subnet automatically has available a set of globally routable source-specific multicast groups for multicast applications

A /48 IPv6 (size of a class B IPv4)

And as my name is “Forrest”,

it’s all about trees!



What are your questions?

Thanks for Listening

David Forrest <mapleparkdevelopment@gmail.com>