Internet Technology and Engineering

Jordan Pyott

2021-05-06

Course Information

Main Topics

- BGP, OSPF, architecture, optimisation with linear programming, Routers, routing protocols `RIP` ect, solving network flow problems

It is expected to go through the booklet in your own time as lectures will be mainly focused on problems within the booklet rather than its main content and learning

> Install CPLEX by IBM student version for solving linear systems

Course Material

Lab Progress **Lab 1**: Got half way through problem 5.3.1

Next step is to populate the config files for both `zebra.conf` and `ripd.conf`

Grades

- Assignment 1 30%
  - Implementing `RIP` routing protocol (we can start this now)
  - Due: Tuesday, April 27th 12:00pm
  - Requirements:
    * Create a report
    * Inspection and showcase of source code and will be marked on showcase
- Assignment 2 15%
  - Due: Wednesday, June 2nd 12:00
- Mid-term test 35%
  - Due: Monday May 3rd 7:00 - 9:00pm
- Take home test (Must pass this to pass course)
  - Due: Monday May 28th 6:00pm
  - On linear programming and simplex computations
- Final exam 20% (One hour)

Both the mid-term and the final exam are closed book tests, however you are permitted to bring a one page hand written cheat sheet on an A4 sheet of paper, double sided.

> NOTE: These assessments will be altered if lock down takes place, see details of adjustment on learn.

Lectures

Lecture One: IPV4 Refresh

Packets are called `dataframes`, each interface in the network is assigned an `IP` address (each wifi card/ethernet)

`IP` service is a *best effort* protocol, it is unreliable, doesn't use acknowledgements, retransmissions etc, here is the packet structure of a `IPV4` packet (dataframe)

packet

Lecture Two: IP Addressing

IP Address Representation

- IP addresses have a width of 32 bits
- They are supposed to be worldwide unique
  - This is no longer true
- IP addresses are written in dotted-decimal notation
- They have an internal structure:
  - `<network-id> <host-id>`

Classless Inter-Domain Routing

- Question: how many bits to allocate to `<network-id>`?
- In the early days this was fixed to three different values
- This proved inflexible
- `CIDR`: Classless Inter-Domain Routing
- Introduced in 1993
- Modern routing protocols `OSPF, RIPv2,` BGP use `CIDR`
- In `CIDR` a network is specified by two values
  - A 32 bit network address
  - A 32 bit network mask (`netmask`)

CIDR - Netmask

- For a given 32-bit IP address, the net-mask specifies which bits belong to network-id and which bit belong to host-id

- The net-mask consists of 32 bits the left *k* bits are ones the remaining 32 - *k* bits are zeros; *where k is the net-mask*

> To use a net-mask in practice we can use a boolean AND operation in order to pull the ones with a mask

In order to completely specify an IP network, we must provide both the IP address and the net-mask:

$$192.168.40.0/24$$

$$192.168.40.0/21$$

> Note: The above network prefixes are NOT the same network. *due to different net-masks*

Aggregation

The number of available host addresses in a `/k` network is: $2^{32-k} - 2$

The big problem is the size of routing/forwarding tables.

Example of why this is a problem: 35:40

Address aggregation is an important approach of reducing the size of forwarding tables, it makes use of `CIDR`. (This keeps the routing tables small)

Lecture Three: IP Forwarding

Routing Daemon

- Refers to the forwarding table
- gathers the IP output
  - deliver directory or calculate next hop
  - decrement `TTL`
  - recompute header checksum
- passed to network interfaces
- IP input queue
- process IP options
- check if our packet:
  - destined to one of my IP addresses
  - destined to broadcast address
    - send via `UDP, TCP, ICMP`
  - Forward datagram *if forwarding is enabled*

Forwarding Table Contents

- Each entry in the forwarding table contains:
  - Destination IP prefix
  - Information about next hop
    * IP address of next-hop router or interface towards it
    * IP address of directly connected network (with net-mask)
  - Flags
    * whether next hop is router or directly attached network
  - Specification of outgoing interface
  - Most end hosts leverage the default route mechanism
    * An end host can differentiate between packets to local destinations
    * Packets to local destinations are delivered directly
    * Packets to all other destinations are sent to default router
- Forwarding tables in Routers
  - Most routers at the fringe of the internet only have routing table entries for a subset of all networks, for all other networks they use default routers
  - Some routers in the core
    * do not have a default router
    * are (transitively) the ultimate default routers of other routers
    * must know (almost) all the internet networks

`ARP Protocol` - Main focus is to find the mac address of a station - Broadcast to the station until a router responds (when the mac address matches the responders)

`ICMP` - Not a protocol, it is just a set of error messages that are useful. - This is optional, you cannot expect a router to implement this as `ICMP` can be stopped with a firewall or by a select router

Lecture Four: Routing Algorithm Structure

The main purpose of this lecture is to discuss the pros and cons of Link State Routing and Distance Vector Routing.

Distance Vector - *Bellman Ford* - Talks only to immediate neighbours. - Once received update, the routers neighbours will re-draw their routing tables. - In `RIP` a triggered update only sends triggered updates when something bad happens (fast). * (`RIP` works on the concept that bad news travels fast and good news travels slow). * Because of this, it may take a long time for nodes in the network to update routing tables + Inconsistencies in routing tables of the network can introduce routing loops. + This can also introduce the counting to infinity problem. + This also introduces security issues as by acting as a node, we can disrupt the neighbouring routing topology

Link State - *Dijkstra's* - Each and every router has a local copy of the full topology on the network (a link state database). - floods changes in the topology to the entire network. - the flood can be fast. - each router hosts its own database. - once the database is up to date, each router runs its algorithm in order to re-allocate the topology of the network. - will need to store a sequence number in order to see whether a router is up to date.

Lecture Five: OSPF

- In OSPF packets get encapsulated
- Distance Vector algorithm (only talks to immediate neighbours)
- is a broadcast network (can reach all stations)
- scalability issue as in large networks many iterations
    - this can be solved with OSPF areas (see lecture 6 and routing-booklet on learn)

OSPF can support five different types of IP sub-networks

- Point-to-point network: OSPF routers are connected through p2p links, only two routers share a transmission medium, and whenever one of them sends there is only one reciever, examples of this include dial-up lines or optical links, in this type of network it is trivial to discover neighboured OSPF routers.
- Broadcast networks: several OSPF routers are attached to an underlying IP subnetwork with MAC-layer broadcast or multicast address and can be heard by all other routers in the same subnetwork, the discovery of all OSPF routers is easy on broadcast networks
- non-broadcast multi-access networks: several OSPF routers are attached to the same IP subnetwork and can reach each other, but this subnetwork does not have broadcast, examples of this type of network is a frame relay network, because of lack of ability to broadcast, finding other routers is difficult.
- virtual links: in virtual links it is possible to connect two non-neighboured OSPF area-border routers through other routers in an intermediate area, intuitively, these two routers establish a tunnel over the intermediate area, and again the discovery of the neighboured router in a virtual link requires configuration.

Lecture Six: OSPF Area's

An aria consists of a number of OSPF routers and IP subnetworks - each IP subnetwork in an OSPF domain belongs to exactly one area. Routers that belong to two different areas are called area-border routers, other routers are called internal routers.

When we have large networks, we have a scalability issue with Distance Vector protocols, because of this we must we would be better to use link state advertisements, this is when a link state advertisement router only generates information about its local environment, (only the attached IP sub-networks and

its neighboured OSPF routers.) Describing an IP subnetwork in an OSPF LSA takes a few tens of bytes, similarly for a neighbour, and considering that usually routers do not have more than a few dozen to a few hundreds of interfaces the total volume of data a router generates for all its links is moderate.

In this type of network, each area can be assigned any ID (no stack template), with one exception, the protocol must contain an area with ID=0. This is called the **backbone area or core area**

- AreaID is identified by a 32-bit value
- OSPF performs hierarchical routing with these areas
- Routers belonging to the core area are called core routers
- Routers pertaining to other areas are called low-level routers as they are apart of low-level area's
- Only the core area can have BGP border routers / AS boundary routers.

Here is the packet structure of the OSPF packet.

packet structure

Lecture Six: OSPF continued; LSA Records

As explained previously, an LSU packet is simply a container for one or more LSA records, therefore the strucutre of an LSA packet is simple (see Routing 3.5)

> NOTE: all fields are set in 32 bits, this is because the data bus size is 32 bits for LSA

Midterm Practice and Information

Link State Routing (OSPF, ISIS) The basics of Link State Routing

Problems seen in distance vector algorithms

- Distance vector protocols converge slowly *good news travels slow*
  - Therefore link state routing is prone to the count to infinity problem

> Packet structure consists of the following knowledge [destination, next_hop, cost]
> the packet does not contain any information about the entire topology of the network

By contrast: in link-state routing each router possesses a local copy of a *link-state database* which contains information about all routers, IP networks reachable through these routers, it also stores the status, current cost, and has a full view of the topology of the network at each point in time.

After each change to the *link-state database* a router performs a local shortest path calculation using the `Dijkstra's Algorithm`, each router also stores the status, cost changes to direct links and their directly attached IP sub-networks / prefixes. This information that is received is known as a `Link State Advertisement (LSA)`.

When a router receives an LSA from a neighbour, it forwards it quickly to its neighbouring routers in order to *flood* the network with information from the advertisement. Each receiving router preforms a routing calculation in order to address its own routing table.

> Routers send LSA's both periodically and upon changes in the link status or upon a change in router cost.

How flooding a network works:

In flooding, a packet originating at a single node is to be disseminated into the entire network (i.e. to all nodes). The process starts by the source node sending the packet to each of its neighbours. A node receiving the packet over some link will, if it sees the packet for the first time, forward it to all its links except the one the packet has been received on. With this approach the packet will eventually reach every node in the network.

Pro's and Con's Distance Vector (RIP)

The distance vector (DV) protocol is the oldest routing protocol in practice. With distance vector routes are advertised based upon the following characteristics:

- Distance - How far the destination network is based upon a metric such as hop count.
- Vector - The direction (next-hop router or egress interface) required to get to the destination.

This routing information is exchanged between directly connected neighbours.[2] Therefore when a node receives a routing update, it has no knowledge of where the neighbour learned it from. In other words, the node has no visibility of the network past its own neighbour. This part of distance vector is also known as "routing by rumour".

Furthermore, routing updates are sent in full (rather than delta-based updates) and at regular intervals, resulting in extremely slow convergence times - one of the key downfalls to distance vector protocols. In addition due to the slow convergence times and "routing by rumour", distance vector protocols are prone to routing loops.

However, on the flipside, the resource consumption is low compared to link-state, due to not having to hold the full state of the entire topology.

Link State (OSPF, ISIS)

In contrast to distance vector routing, link state routing (OSPF, ISIS) relies on each node advertising/flooding the state (i.e. delay, bandwidth etc) of their links to every node within the link state domain. This results in each node building a complete map of the network (shortest path tree), with itself as the root using the shortest path first algorithm, also known as the Dijkstra algorithm.

Unlike distance vector link-state neighbours only sends incremental routing updates (LSAs) rather than a full routing update. Also, these updates are only sent at the point a change in the network topology occurs, rather than at regular intervals.

Link-state protocols provide extremely low convergence times and, due to each router having a complete view of the network, aren't prone to the same routing loops seen with DV-based protocols.

However, due to the computation required for the algorithms to run across the shortest path trees upon each node, greater resources are consumed compared to that of distance vector, however, this really isn't a concern with the systems of today.

Path Vector (BGP)

Path vector (PV) protocols, such as BGP, are used across domains aka autonomous systems. In a path vector protocol, a router does not just receive the distance vector for a particular destination from its neighbor; instead, a node receives the distance as well as path information (aka BGP path attributes), that the node can use to calculate (via the BGP path selection process) how traffic is routed to the destination AS.

Hybrid (EIGRP)

A hybrid routing protocol consists of characteristics from both, link state and distance vector routing protocols.

For example, EIGRP can be considered a hybrid routing protocol, as it displays characters of both. As shown below:

Distance Vector	Link State
EIGRP routers only advertise the best route , not every route that is aware of.	An EIGRP router forms neighbour relationships.
EIGRP routers do not have a complete network map of the topology, but only what it has been told by its neighbour aka "routing by rumour".	Triggered updates are sent only when a topology change occurs.