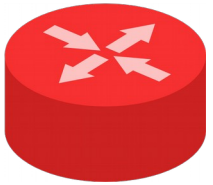
Formal verification of an LPM data structure

Bachelor project, DSLAB
Simon Perriard



Content

1. LPM data structure
2. DIR-24-8-BASIC
3. Formal representations in VeriFast

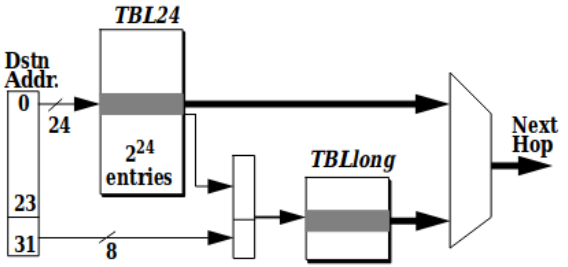
1. LPM data structure

- DIR-24-8-BASIC

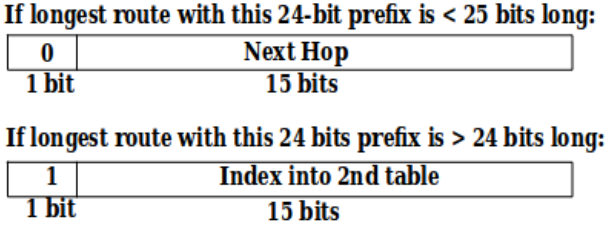
- P. Gupta, St. Lin and N. McKeown.
  “Routing Lookups in Hardware at Memory Access Speeds.”
  Proc. IEEE INFOCOM 1998, Computer Systems Laboratory,
  Standford University.

2. DIR-24-8-BASIC

- TBL24: 2^{24} entries
- TBLlong: 2^{16} entries
- 0 <= next hop < 0xFFFF
- 0 <= index into 2nd table <= 0xFF
- Index in TBL24: 24 MSB
- Index in TBLlong:
  256 * (index into 2nd table) + 8 LSB



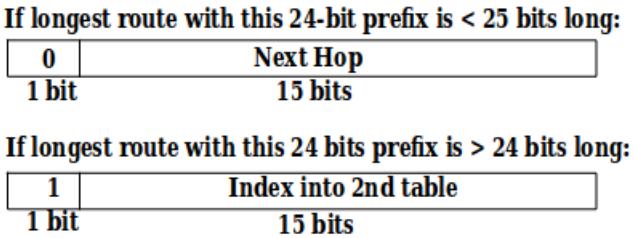
Hardware architecture model



TBL24 entry format

3.1 DS formal representation

- TBL24: list<option<pair<bool, Z> > >
- TBLlong: list<option<Z> >
- Z: integer binary representation
- DS held in dir(TBL24, TBLlong, next index long to be used)



TBL24 entry format

3.2 Lookup formal representation

```
fixpoint int lpm_dir_24_8_lookup(Z ipv4, dir_24_8 dir){
  switch(dir){
    case tables(lpm_24, lpm_long, index_long): return
      switch(lookup_lpm_24(index24_from_ipv4(ipv4), dir)){
        case none: return 0xFFFF;
        case some(p): return
          switch(p){
            case pair(f, v): return
              f ?
                switch(lookup_lpm_long(indexlong_from_ipv4(ipv4,
                    int_of_Z(v)), dir))
                {
                  case none: return 0xFFFF;
                  case some(vl): return int_of_Z(vl);
                }
              :
                int_of_Z(v);
          };
      };
  }
}
```

3.3 Update formal representation (1)

```
fixpoint dir_24_8 add_rule(dir_24_8 dir, lpm_rule rule){
  switch(rule){
    case rule(ipv4, prefixlen, route):
      return prefixlen < 25 ?
               insert_lpm_24(dir, rule)
             :
               insert_lpm_long(dir, rule);
  }
}

fixpoint dir_24_8 insert_lpm_24(dir_24_8 dir, lpm_rule rule){
  switch(dir){
    case tables(lpm_24, lpm_long, long_index):
      return tables(insert_route_24(lpm_24, rule), lpm_long, long_index);
  }
}
```

3.3 Update formal representation (2)

```
fixpoint dir_24_8 insert_lpm_long(dir_24_8 dir, lpm_rule rule){
  switch(dir){
    case tables(lpm_24, lpm_long, long_index): return
      switch(rule){
        case rule(ipv4, prefixlen, route): return
          //Check whether a new index_long is needed
          is_new_index_needed(lookup_lpm_24(index24_from_ipv4(ipv4),
              dir)) ?
            //Check for available index, if not -> no change
            long_index == 256 ?
              tables(lpm_24, lpm_long, long_index)
            :
              //Update the value in lpm_24 and lpm_long
              tables(update_n(lpm_24, compute_starting_index_24(rule),
                              N1,
                              some(pair(true,
                                        Z_of_int(long_index, N16)))),
                     insert_route_long(lpm_long, rule, long_index),
                     long_index + 1)
          :
            //No need to update the value in lpm_24, only in tlb_long
            tables(lpm_24,
                   insert_route_long(lpm_long, rule,
                                     extract24_value(lookup_lpm_24(index24_from_ipv4(ipv4),
                                     dir))),
                   long_index);
      };
  }
}
```

Questions ?