LOFT — Verified Migration of Linux Firewalls to SDN

Julius Michaelis and Cornelius Diekmann

April 20, 2020

Abstract

We present LOFT — Linux firewall OpenFlow Translator, a system that transforms the main routing table and FORWARD chain of iptables of a Linux-based firewall into a set of static OpenFlow rules. Our implementation is verified against a model of a simplified Linux-based router and we can directly show how much of the original functionality is preserved.

Please note that this document is organized in two distinct parts. The first part contains the necessary definitions, helper lemmas and proofs in all their technicality as made in the theory code. The second part reiterates the most important definitions and proofs in a manner that is more suitable for human readers and enriches them with detailed explanations in natural language. Any interested reader should start from there.

Many of the considerations that have led to the definitions made here have been explained in [8].

Contents

I Code 2

II Documentation 44

1 Configuration Translation 44

1.1 Linux Firewall Model ................................................................. 44

1.1.1 Routing Table ................................................................... 45

1.1.2 iptables Firewall ................................................................. 46

1.2 OpenFlow Switch Model ............................................................ 46

1.2.1 Matching Flow Table entries .............................................. 47

1.2.2 Evaluating a Flow Table ....................................................... 47

1.3 Translation Implementation ....................................................... 49

1.3.1 Chaining Firewalls .............................................................. 49

1.3.2 Translation Implementation .................................................. 50

1.3.3 Comparison to Exodus ......................................................... 52

2 Evaluation 52

2.1 Mininet Examples ................................................................... 52

2.2 Performance Evaluation ........................................................... 54

3 Conclusion and Future Work 55
Part I

Code

theory OpenFlow-Matches
imports IP-Addresses.Prefix-Match
  Simple-Firewall.Simple-Packet
  HOL-Library.Monad-Syntax
  HOL-Library.List-Lexorder
  HOL-Library.Char-ord

begin

datatype of-match-field =
  IngressPort string
| EtherSrc 48 word
| EtherDst 48 word
| EtherType 16 word
| VlanId 16 word
| VlanPriority 16 word
| IPv4Src 32 prefix-match
| IPv4Dst 32 prefix-match
| IPv4Proto 8 word
| L4Src 16 word 16 word
| L4Dst 16 word 16 word

schematic-goal of-match-field-typeset: (field-match :: of-match-field) ∈ {
  IngressPort (?s::string),
  EtherSrc (?as::48 word), EtherDst (?ad::48 word),
  EtherType (?t::16 word),
  VlanId (?i::16 word), VlanPriority (?p::16 word),
  IPv4Src (?pms::32 prefix-match), IPv4Dst (?pmd::32 prefix-match),
  IPv4Proto (?ipp :: 8 word),
  L4Src (?ps :: 16 word) (?ms :: 16 word),
  L4Dst (?pd :: 16 word) (?md :: 16 word)
}

proof((cases field-match;clarsimp),goal-cases)
  next case (IngressPort s)  thus s = (case field-match of IngressPort s ⇒ s) unfolding IngressPort of-match-field.simps by rule
  next case (EtherSrc s)    thus s = (case field-match of EtherSrc s ⇒ s) unfolding EtherSrc of-match-field.simps by rule
  next case (EtherDst s)    thus s = (case field-match of EtherDst s ⇒ s) unfolding EtherDst of-match-field.simps by rule
  next case (EtherType s)   thus s = (case field-match of EtherType s ⇒ s) unfolding EtherType of-match-field.simps by rule
  next case (VlanId s)      thus s = (case field-match of VlanId s ⇒ s) unfolding VlanId of-match-field.simps by rule
  next case (VlanPriority s) thus s = (case field-match of VlanPriority s ⇒ s) unfolding VlanPriority of-match-field.simps by rule
}
next case (IPv4Src s) thus s = (case field-match of IPv4Src s ⇒ s) unfolding IPv4Src of-match-field.simps by rule
next case (IPv4Dst s) thus s = (case field-match of IPv4Dst s ⇒ s) by simp
next case (IPv4Proto s) thus s = (case field-match of IPv4Proto s ⇒ s) by simp
next case (IPv4Src p l) thus p = (case field-match of IPv4Src p l ⇒ p) ∧ l = (case field-match of IPv4Src p l ⇒ l) by simp
next case (IPv4Dst p l) thus p = (case field-match of IPv4Dst p l ⇒ p) ∧ l = (case field-match of IPv4Dst p l ⇒ l) by simp
qed

function prerequisites :: of-match-field ⇒ of-match-field set ⇒ bool where
prerequisites (IngressPort -) - = True |
prerequisites (EtherDst -) - = True |
prerequisites (EtherSrc -) - = True |
prerequisites (EtherType -) - = True |
prerequisites (VlanId -) - = True |
prerequisites (VlanPriority -) m = (∃ id. let v = VlanId id in v ∈ m ∧ prerequisites v m) |
prerequisites (IPv4Proto -) m = (let v = EtherType 0x0800 in v ∈ m ∧ prerequisites v m) |
prerequisites (IPv4Src -) m = (let v = EtherType 0x0800 in v ∈ m ∧ prerequisites v m) |
prerequisites (IPv4Dst -) m = (let v = EtherType 0x0800 in v ∈ m ∧ prerequisites v m) |
prerequisites (IPv4Src -) m = (∃ id. let v = VlanId id in v ∈ m ∧ prerequisites v m) |
prerequisites (IPv4Dst -) m = prerequisites (IPv4Src undefined undefined) m by pat-completeness auto

fun match-sorter :: of-match-field ⇒ nat where
match-sorter (IngressPort -) = 1 |
match-sorter (VlanId -) = 2 |
match-sorter (VlanPriority -) = 3 |
match-sorter (EtherType -) = 4 |
match-sorter (EtherSrc -) = 5 |
match-sorter (EtherDst -) = 6 |
match-sorter (IPv4Proto -) = 7 |
match-sorter (IPv4Src -) = 8 |
match-sorter (IPv4Dst -) = 9 |
match-sorter (IPv4Src -) = 10 |
match-sorter (IPv4Dst -) = 11

termination prerequisites by(relation measure (match-sorter ◦ fst), simp-all)
definition less-eq-of-match-field1 :: of-match-field ⇒ of-match-field ⇒ bool
where \text{less-eq-of-match-field1} \ (a::\text{of-match-field}) \ (b::\text{of-match-field}) \iff \text{(case} (a, b) \text{ of)}
\begin{align*}
(\text{IngressPort} \ a, \text{IngressPort} \ b) & \Rightarrow a \leq b \ | \\
(\text{VlanId} \ a, \text{VlanId} \ b) & \Rightarrow a \leq b \ | \\
(\text{EtherDst} \ a, \text{EtherDst} \ b) & \Rightarrow a \leq b \ | \\
(\text{EtherSrc} \ a, \text{EtherSrc} \ b) & \Rightarrow a \leq b \ | \\
(\text{EtherType} \ a, \text{EtherType} \ b) & \Rightarrow a \leq b \ | \\
(\text{VlanPriority} \ a, \text{VlanPriority} \ b) & \Rightarrow a \leq b \ | \\
(\text{IPv4Proto} \ a, \text{IPv4Proto} \ b) & \Rightarrow a \leq b \ | \\
(\text{IPv4Src} \ a, \text{IPv4Src} \ b) & \Rightarrow a \leq b \ | \\
(\text{IPv4Dst} \ a, \text{IPv4Dst} \ b) & \Rightarrow a \leq b \ | \\
(\text{L4Src} \ a1 a2, \text{L4Src} \ b1 b2) & \Rightarrow \text{if} \ a2 = b2 \ \text{then} \ a1 \leq b1 \ \text{else} \ a2 \leq b2 \ | \\
(\text{L4Dst} \ a1 a2, \text{L4Dst} \ b1 b2) & \Rightarrow \text{if} \ a2 = b2 \ \text{then} \ a1 \leq b1 \ \text{else} \ a2 \leq b2 \ | \\
(a, b) & \Rightarrow \text{match-sorter} \ a < \text{match-sorter} \ b
\end{align*}

\text{instantiation} \ \text{of-match-field} :: \text{linorder}

\text{begin}

\text{definition} \ \text{less-eq-of-match-field (a::of-match-field) (b::of-match-field) \iff less-eq-of-match-field1 a b}

\text{definition} \ \text{less-of-match-field (a::of-match-field) (b::of-match-field) \iff a \neq b \land less-eq-of-match-field1 a b}

\text{instance} \ \text{by standard (auto simp add: less-eq-of-match-field-def less-of-match-field-def less-eq-of-match-field1-def split: prod.splits of-match-field.splits if-splits)}

\text{end}

\text{fun} \ \text{match-no-prereq :: of-match-field \Rightarrow (32,'a) simple-packet-ext-scheme \Rightarrow bool where}
\begin{align*}
\text{match-no-prereq (IngressPort \ i) \ p} & = (p-iface \ p = i) \ | \\
\text{match-no-prereq (EtherDst \ i) \ p} & = (p-l2src \ p = i) \ | \\
\text{match-no-prereq (EtherSrc \ i) \ p} & = (p-l2dst \ p = i) \ | \\
\text{match-no-prereq (EtherType \ i) \ p} & = (p-l2type \ p = i) \ | \\
\text{match-no-prereq (VlanId \ i) \ p} & = (p-vlanid \ p = i) \ | \\
\text{match-no-prereq (VlanPriority \ i) \ p} & = (p-vlanprio \ p = i) \ | \\
\text{match-no-prereq (IPv4Proto \ i) \ p} & = (p-protocol \ p = i) \ | \\
\text{match-no-prereq (IPv4Src \ i) \ p} & = (p-prefix-match-semantics (p-src \ p)) \ | \\
\text{match-no-prereq (IPv4Dst \ i) \ p} & = (p-prefix-match-semantics (p-dst \ p)) \ | \\
\text{match-no-prereq (L4Src \ i \ m) \ p} & = (p-sport \ p \&\& \ m = i) \ | \\
\text{match-no-prereq (L4Dst \ i \ m) \ p} & = (p-dport \ p \&\& \ m = i)
\end{align*}

\text{definition} \ \text{match-prereq :: of-match-field \Rightarrow of-match-field set \Rightarrow (32,'a) simple-packet-ext-scheme \Rightarrow bool option where}
\begin{align*}
\text{match-prereq} \ i \ s \ p & = (\text{if prerequisites} \ i \ s \ \text{then} \ Some \ (\text{match-no-prereq} \ i \ p) \ \text{else} \ None)
\end{align*}

\text{definition} \ \text{set-seq} \ s \equiv (\forall \ x \in \ s. \ x \neq None) \ \text{then} \ Some \ (\text{the} \ 's) \ \text{else} \ None

\text{definition} \ \text{all-true} \ s \equiv \forall \ x \in \ s. \ x

\text{term} \ \text{map-option}

\text{definition} \ \text{OF-match-fields :: of-match-field set \Rightarrow (32,'a) simple-packet-ext-scheme \Rightarrow bool option where}
\begin{align*}
\text{OF-match-fields} \ m \ p & = \text{map-option all-true} \ \text{(set-seq (\lambda f. match-prereq f m p) \ 'm))}
\end{align*}

\text{definition} \ \text{OF-match-fields-unsafe :: of-match-field set \Rightarrow (32,'a) simple-packet-ext-scheme \Rightarrow bool where}
\begin{align*}
\text{OF-match-fields-unsafe} \ m \ p & = (\forall f \in \ m. \ \text{match-no-prereq} \ f \ p)
\end{align*}

\text{definition} \ \text{OF-match-fields-safe} \ m \equiv \forall \ \text{OF-match-fields} \ m
definition all-prerequisites $m \equiv \forall f \in m. \text{prerequisites } f m$

lemma
all-prerequisites $p \implies$
$L4\text{Src } x y \in p \implies$
$IPec\text{Proto } \{TCP, UDP, L4-Protocol.SCTP\} \cap p \neq \{\}$

unfolding all-prerequisites-def by auto

lemma of-safe-unsafe-match-eq: all-prerequisites $m \implies\text{OF-match-fields } m p = \text{Some (OF-match-fields-unsafe } m p)$
unfolding OF-match-fields-def OF-match-fields-unsafe-def comp-def set-seq-def match-prereq-def all-prerequisites-def
proof goal-cases
  case 1
  have 2: $(\lambda f. \text{if prerequisites } f m \text{ then Some (match-no-prereq } f p) \text{ else None }) \ ' m = (\lambda f. \text{Some (match-no-prereq } f p)) \ ' m$
  using 1 by fastforce
  have 3: $\forall x \in (\lambda f. \text{Some (match-no-prereq } f p) \ ' m. x \neq \text{None } \text{by blast}$
  show \text{case}
  unfolding 2 unfolding eqTrueI [OF 3] unfolding if-True unfolding image-comp comp-def unfolding option.sel by(simp add: all-true-def)
  qed

lemma of-match-fields-safe-eq: assumes all-prerequisites $m$ shows OF-match-fields-safe $m p = \text{OF-match-fields-unsafe } m p$

lemma OF-match-fields-alt: OF-match-fields $m p =$
(if $\exists f \in m. \neg \text{prerequisites } f m$ then None else
  if $\forall f \in m. \text{match-no-prereq } f p$ then Some True else Some False)
unfolding OF-match-fields-def all-true-def set-seq-def match-prereq-def
by(auto simp add: ball-Un)

lemma of-match-fields-safe-eq2: assumes all-prerequisites $m$ shows OF-match-fields-safe $m p \longleftrightarrow \text{OF-match-fields } m p = \text{Some True}$

end
theory OpenFlow-Action
imports
OpenFlow-Matches
begin

datatype of-action = Forward (oiface-sel: string) | ModifyField-l2dst 48 word

fun of-action-semantics where
of-action-semantics $p [] = \{\}$ |
of-action-semantics $p (a\#as) = \text{(case } a \text{ of}
value of-action-semantics p [ModifyField-l2dst a] as [value of-action-semantics p]

end
theory Semantics-OpenFlow
imports List-Group Sort-Descending
IP-Addresses.IPV4
OpenFlow-Helpers
begin

datatype 'a flowtable-behavior = Action 'a | NoAction | Undefined

definition option-to-ftb b ≡ case b of Some a ⇒ Action a | None ⇒ NoAction

definition ftb-to-option b ≡ case b of Action a ⇒ Some a | NoAction ⇒ None

datatype ('m, 'a) flow-entry-match = OFEntry (ofe-prio: 16 word) (ofe-fields: 'm set) (ofe-action: 'a)

find-consts (('a × 'b) ⇒ 'c) ⇒ ('a ⇒ 'b ⇒ 'c)

find-consts ('a ⇒ 'b ⇒ 'c) ⇒ ('a × 'b) ⇒ 'c

definition split3 f p ≡ case p of (a,b,c) ⇒ f a b c

find-consts ('a ⇒ 'b ⇒ 'c ⇒ 'd) ⇒ ('a × 'b × 'c) ⇒ 'd

type-synonym ('m, 'a) flowtable = ('m, 'a) flow-entry-match list

type-synonym ('m, 'p) field-matcher = ('m set ⇒ 'p ⇒ bool)

definition OF-same-priority-match2 :: ('m, 'p) field-matcher ⇒ ('m, 'a) flowtable ⇒ 'p ⇒ 'a flowtable-behavior where

OF-same-priority-match2 γ flow-entries packet ≡ let s =
{(ofe-action f | f ∈ set flow-entries ∧ γ (ofe-fields f) packet ∧
(∀ fo ∈ set flow-entries. ofe-prio fo > ofe-prio f −> ¬γ (ofe-fields fo) packet))} in

case card s of 0 ⇒ NoAction
| (Suc 0) ⇒ Action (the-elem s)
| - ⇒ Undefined
definition check-no-overlap \( \gamma \ ft = (\forall a \in \text{set ft.} \ \forall b \in \text{set ft.} \ \forall p \in \text{UNIV.} \ \text{ofe-prio a = ofe-prio b} \land \gamma \ (\text{oefe-fields a} \ p \land \ a \neq b) \rightarrow \neg \gamma \ (\text{oefe-fields b} \ p) \)

definition check-no-overlap2 \( \gamma \ ft = (\forall a \in \text{set ft.} \ \forall b \in \text{set ft.} \ (a \neq b \land \text{ofe-prio a = ofe-prio b}) \rightarrow \neg (\exists p \in \text{UNIV.} \ \gamma \ (\text{oefe-fields a} \ p \land \gamma \ (\text{oefe-fields b} \ p)) \)

lemma check-no-overlap-alt: check-no-overlap \( \gamma \ ft = \text{check-no-overlap2} \ \gamma \ ft \)

unfolding check-no-overlap2-def check-no-overlap-def

by blast

lemma no-overlap-not-undefined: check-no-overlap \( \gamma \ ft \Rightarrow \text{OF-same-priority-match2} \ \gamma \ ft \ p \neq \text{Undefined} \)

proof
assume goal1: check-no-overlap \( \gamma \ ft \) \text{OF-same-priority-match2} \( \gamma \ ft \ p = \text{Undefined} \)

let \( ?as = \{f : f \in \text{set ft} \land \gamma \ (\text{oefe-fields f} \ p) \land (\forall fo \in \text{set ft.} \ \text{ofe-prio f} < \text{ofe-prio fo} \rightarrow \neg \gamma \ (\text{oefe-fields fo} \ p)) \} \)

have fin: finite \( ?as \) by simp

note goal1(2)[unfolded \text{OF-same-priority-match2-def}]

then have \( 2 \leq \text{card (oefe-action ' ?as)} \) unfolding f-img-ex-set

unfolding Let-def

by(cases \( \text{card (oefe-action ' ?as)} \), simp) (rename-tac nat1, case-tac nat1, simp add: image-Collect, presburger)

then have \( 2 \leq \text{card ?as} \) using \( \text{OF_fin} \), \( \text{ofe-action a} \) by linarith

then obtain \( a \ b \ ) where \( \text{ab:} a \neq b \ a \in ?as \ b \in ?as \ using \text{card2-El} \ ) by blast

then have \( \text{ab2:} a \in \text{set ft} \ \gamma \ (\text{oefe-fields a} \ p) \ (\forall fo \in \text{set ft.} \ \text{ofe-prio a < ofe-prio fo} \rightarrow \neg \gamma \ (\text{oefe-fields fo} \ p)) \)

\( b \in \text{set ft} \ \gamma \ (\text{oefe-fields b} \ p) \ (\forall fo \in \text{set ft.} \ \text{ofe-prio b < ofe-prio fo} \rightarrow \neg \gamma \ (\text{oefe-fields fo} \ p)) \) by simp-all

then have \( \text{oefe-prio a = ofe-prio b} \)

by fastforce

note goal1(1)[unfolded check-no-overlap-def] \( \text{ab2(1) ab2(4) this ab2(2) ab(1) ab2(5)} \)

then show False by blast

qed

fun \( \text{OF-match-linear :: ('}m', 'p') \) \text{field-matcher \Rightarrow ('}m', 'a') \) \text{flowtable \Rightarrow 'p \Rightarrow 'a flowtable-behavior where}

\( \text{OF-match-linear} : [ ] = \text{NoAction |} \)

\( \text{OF-match-linear} \ (a \# as) = \text{if (} \gamma \ (\text{oefe-fields a}) \ p) \ \text{then Action (oefe-action a) else OF-match-linear} \) as p)

lemma \( \text{OF-match-linear-ne-Undefined: OF-match-linear} \ \gamma \ ft \ p \neq \text{Undefined} \)

by(induction ft) auto

lemma \( \text{OF-match-linear-append: OF-match-linear} \ \gamma (a \ @ b) \ p = \text{(case OF-match-linear} \ \gamma (a \ p) \ \text{of NoAction \Rightarrow} \)

\( \text{OF-match-linear} \ b \ p \mid x \Rightarrow x) \)

by(induction a) simp-all

lemma \( \text{OF-match-linear-match-allsameaction:} [gr \in \text{set oms; } \gamma \ gr \ p = \text{True}] \)

\( \Rightarrow \text{OF-match-linear} \ \gamma \ (\text{map (}\lambda x. \text{split3 OFEntry (pri, x, act))} \) oms \ p) = \text{Action act} \)

by(induction oms) (auto simp add: split3-def)

lemma \( \text{OF-lm-noa-none-iff: OF-match-linear} \ \gamma \ ft \ p = \text{NoAction} \ \iff \ (\forall e \in \text{set ft.} \ \neg \gamma (\text{oefe-fields} e) \ p) \)

by(induction ft) (simp-all split: if-splits)

lemma set-eq-rule: \( (\lambda x. \ x \in a \Rightarrow x \in b) \Rightarrow (\lambda x. x \in b \Rightarrow x \in a) \Rightarrow a = b \) by(rule antisym[OF subsetI subsetI])

lemma unmatching-insert-agnostic: \( \neg \gamma (\text{oefe-fields} a) \ p \ \Rightarrow \text{OF-same-priority-match2} \ \gamma (a \neq ft) \ p = \text{OF-same-priority-match2} \gamma \ ft \ p \)

proof

let \( ?as = \{f : f \in \text{set ft} \land \gamma \ (\text{oefe-fields f} \ p) \land (\forall fo \in \text{set ft.} \ \text{ofe-prio f < ofe-prio fo} \rightarrow \neg \gamma (\text{oefe-fields fo} \ p)) \} \)

let \( ?aas = \{f | f \in \text{set (a \neq ft)} \land \gamma (\text{oefe-fields f} \ p) \land (\forall fo \in \text{set} (a \neq ft). \ \text{ofe-prio f < ofe-prio fo} \rightarrow \neg \gamma (\text{oefe-fields fo} \ p)) \} \)

assume nm: \( \neg \gamma (\text{oefe-fields a}) \ p \)

7
have aa: ?aas = ?as
proof (rule set-eq-rule)
  fix x
  assume x ∈ {f ∈ set (a ≠ ft) ∧ γ (ofe-fields f) p ∧ (∀ f ∈ set (a ≠ ft). ofe-prio f < ofe-prio fo → ¬ γ (ofe-fields fo) p)}
  hence as: x ∈ set (a ≠ ft) ∧ γ (ofe-fields x) p ∧ (∀ f ∈ set (a ≠ ft). ofe-prio x < ofe-prio fo → ¬ γ (ofe-fields fo) p)
  by simp
  with nm have x ∈ set ft by fastforce
  moreover from as have (∀ f ∈ set ft. ofe-prio x < ofe-prio fo → ¬ γ (ofe-fields fo) p) by simp
  ultimately show x ∈ {f ∈ set ft. γ (ofe-fields x) p ∧ (∀ f ∈ set ft. ofe-prio f < ofe-prio fo → ¬ γ (ofe-fields fo) p)}
  using as by force
next
  fix x
  assume x ∈ {f ∈ set ft. γ (ofe-fields f) p ∧ (∀ f ∈ set ft. ofe-prio f < ofe-prio fo → ¬ γ (ofe-fields fo) p)}
  hence as: x ∈ set ft γ (ofe-fields x) p ∧ (∀ f ∈ set ft. ofe-prio x < ofe-prio fo → ¬ γ (ofe-fields fo) p) by simp-all
  from as(1) have x ∈ set (a ≠ ft) by simp
  moreover from as(3) have (∀ f ∈ set (a ≠ ft). ofe-prio x < ofe-prio fo → ¬ γ (ofe-fields fo) p) using nm by simp
  ultimately show x ∈ {f ∈ set ft. γ (ofe-fields f) p ∧ (∀ f ∈ set ft. ofe-prio f < ofe-prio fo → ¬ γ (ofe-fields fo) p)} using as(2) by blast
qed

note uf = arg-cong[OF aa, of (') of-action, unfolded image-Collect]
show ?thesis unfolding OF-same-priority-match2-def using af by presburger
qed

lemma OF-match-eq: sorted-descending (map ofe-prio ft) ⇒ check-no-overlap γ ft ⇒
OF-same-priority-match2 γ ft p = OF-match-linear γ ft p
proof (induction ft)
case (Cons a ft)
  have 1: sorted-descending (map ofe-prio ft) using Cons(2) by simp
  have 2: check-no-overlap γ ft using Cons(3) unfolding check-no-overlap-def using set-subset-Cons by fast
  note mIH = Cons(1)(OF 1 2]
  show ?case is ?kees
  proof (cases (γ (ofe-fields a) p)
    case False thus ?kees
    by (simp only: OF-match-linear.simps if-False mIH[symmetric] unmatching-insert-agnostic[of γ, OF False])
next
  note sorted-descending-split[OF Cons(2)]
  then obtain mn wheremn: a ≠ ft = m @ n ∀ e ∈ set m. ofe-prio a = ofe-prio e ∧ ∀ e ∈ set n. ofe-prio e < ofe-prio a
  unfolding list.sel by blast
  hence aem: a ∈ set m
    by (metis UnE less-imp-neq list.intros(1) set.append)
  have mover: check-no-overlap γ m using Cons(3) unfolding check-no-overlap-def
    by (metis Un_iff mn(1) set.append)
  let ?fc = (λs. {f ∈ set s ∧ γ (ofe-fields f) p ∧ (∀ f ∈ set (a ≠ ft). ofe-prio f < ofe-prio fo → ¬ γ (ofe-fields fo) p)}
    case True
  have ?fc (m @ n) = ?fc m ∪ ?fc n by auto
  moreover have ?fc n = {}
  proof (rule set-eq-rule, rule contr, goal-cases)
    case (1 x)
    hence g1: x ∈ set n γ (ofe-fields x) p
      (∀ f ∈ set m. ofe-prio x < ofe-prio fo → ¬ γ (ofe-fields fo) p)
      (∀ f ∈ set n. ofe-prio x < ofe-prio fo → ¬ γ (ofe-fields fo) p)
unfolding \( mn(1) \) by \( \text{simp-all} \)
from \( g1(1) \) \( mn(3) \) have le: ofe-prio \( x < \) ofe-prio \( a \) by \( \text{simp} \)
note le \( g1(3) \) aem True
then show False by blast
qed simp
ultimately have \( cc: \?fc (m \otimes n) = \?fc m \) by \( \text{blast} \)
have cm: \( \?fc m = \{a\} \)
proof –
  have \( \forall f \in \text{set } m. (\forall fo \in \text{set } (a \# ft). \text{ofe-prio } f < \text{ofe-prio } fo \implies \neg \gamma (\text{ofe-fields } fo) p) \)
    by (\text{metis UnE less-asym } mn \text{ set-append})
  hence \( I: \?fc m = \{f \in \text{set } m. \gamma (\text{ofe-fields } f) p\} \) by \( \text{blast} \)
  show \( \{f \in \text{set } m. \gamma (\text{ofe-fields } f) p \wedge (\forall fo \in \text{set } (a \# ft). \text{ofe-prio } f < \text{ofe-prio } fo \implies \neg \gamma (\text{ofe-fields } fo) p)\} = \{a\} \)
unfolding \( I \)
proof (\text{rule set-eq-rule, goal-cases fwd bwd})
  case (bwd \( x \))
    have \( a \in \{f \in \text{set } m. \gamma (\text{ofe-fields } f) p\} \) using True aem by \( \text{simp} \)
    thus ?case using bwd by \( \text{simp} \)
  next
    case (fwd \( x \))
    show ?case proof (\text{rule ccontr})
      assume \( x \not\in \{a\} \) hence \( x \not= a \) by \( \text{simp} \)
      from fwd have \( 1: x \in \text{set } m. \gamma (\text{ofe-fields } x) p \) by \( \text{simp-all} \)
      have \( 2: \text{ofe-prio } x = \text{ofe-prio } a \) using \( 1(1) \) \( mn(2) \) by \( \text{simp} \)
      show False using \( 1 \) ne mover aem True \( 2 \) unfolding check-no-overlap-def by \( \text{blast} \)
    qed
  qed
  qed
  show \( ??ees \)
  unfolding \( mn(1) \)
  unfolding \( \text{OF-same-priority-match2-def} \)
  unfolding \( f\text{-Img-ex-set} \)
  unfolding \( \text{cc[unfolded } mn(1)\text{]} \)
  unfolding \( \text{cm[unfolded } mn(1)\text{]} \)
  unfolding \( \text{Let-def} \)
    by (\text{simp only: } mn(1)[\text{symmetric}] \text{ OF-match-linear.simps True if-True, simp})
  qed
qed (\text{simp add: } \text{OF-same-priority-match2-def})
lemma overlap-sort-invar [simp]: check-no-overlap \( \gamma (\text{sort-descending-key } k \text{ ft}) = \text{check-no-overlap } \gamma \text{ ft} \)
unfolding check-no-overlap-def
unfolding sort-descending-set-inv
.. 

lemma \( \text{OF-match-eq2:} \)
  assumes \( \text{check-no-overlap } \gamma \text{ ft} \)
  shows \( \text{OF-same-priority-match2 } \gamma \text{ ft } p = \text{OF-match-linear } \gamma (\text{sort-descending-key ofe-prio ft}) p \)
proof –
  have \( \text{sorted-descending } (\text{map ofe-prio } (\text{sort-descending-key ofe-prio ft})) \) by (\text{simp add: sorted-descending-sort-descending-key})
  note ceq = \( \text{OF-match-eq}(\text{OF this, unfolded overlap-sort-invar, OF (check-no-overlap } \gamma \text{ ft), symmetric}) \)
  show ?thesis
  unfolding ceq
  unfolding \( \text{OF-same-priority-match2-def} \)
  unfolding sort-descending-set-inv
  ..
```
qed

lemma prio-match-matcher-alt: {f. f ∈ set flow-entries ∧ γ (ofe-fields f) packet ∧ 
(∀ fo ∈ set flow-entries. ofe-prio fo > ofe-prio f → ¬γ (ofe-fields fo) packet)}
= ( 
let matching = {f. f ∈ set flow-entries ∧ γ (ofe-fields f) packet}
in {f. f ∈ matching ∧ (∀ fo ∈ matching. ofe-prio fo ≤ ofe-prio f)}
) 
by(auto simp add: Let-def)

lemma prio-match-matcher-alt2: ( 
let matching = {f. f ∈ set flow-entries ∧ γ (ofe-fields f) packet}
in {f. f ∈ matching ∧ (∀ fo ∈ matching. ofe-prio fo ≤ ofe-prio f)}
) = set ( 
let matching = filter (λf. γ (ofe-fields f) packet) flow-entries 
in filter (λf. ∀ fo ∈ set matching. ofe-prio fo ≤ ofe-prio f) matching 
) 
by(auto simp add: Let-def)

definition OF-priority-match where
OF-priority-match γ flow-entries packet ≡
let m = filter (λf. γ (ofe-fields f) packet) flow-entries;
  m' = filter (λf. ∀ fo ∈ set m. ofe-prio fo ≤ ofe-prio f) m in
case m' of [] ⇒ NoAction 
  | [s] ⇒ Action (ofe-action s) 
  | _ ⇒ Undefined

definition OF-priority-match-ana where
OF-priority-match-ana γ flow-entries packet ≡
let m = filter (λf. γ (ofe-fields f) packet) flow-entries;
  m' = filter (λf. ∀ fo ∈ set m. ofe-prio fo ≤ ofe-prio f) m in
case m' of [] ⇒ NoAction 
  | [s] ⇒ Action s 
  | _ ⇒ Undefined

lemma filter-singleton: [x←. f x] = [y] =⇒ f y ∧ y ∈ set s by (metis filter-eq-Cons-iff in-set-conv-decomp)

unfolding OF-priority-match-def OF-priority-match-ana-def
by(clarsimp split: flowtable-behavior.splits list.splits) (erule filter-singleton; simp)

fun no-overlaps where
no-overlaps - [] = True | 
no-overlaps γ (a#as) = (no-overlaps γ as ∧ ( 
  ∀ b ∈ set as. ofe-prio a = ofe-prio b →¬(∃ p ∈ UNIV. γ (ofe-fields a) p ∧ γ (ofe-fields b) p)))

lemma no-overlap-ConsI: check-no-overlap2 γ (x#xs) =⇒ check-no-overlap2 γ xs
unfolding check-no-overlap2-def by simp

lemma no-overlapsI: check-no-overlap γ t =⇒ distinct t =⇒ no-overlaps γ t
unfolding check-no-overlap-alt

proof(induction t)
  case (Cons a t)
```
from no-overlap-Cons1[OF Cons(2)] Cons(3,1)

have no-overlaps \gamma t by simp
thus \case using Cons(2,3) unfolding check-no-overlap2-def by auto

qed (simp add: check-no-overlap2-def)


lemma check-no-overlapI: no-overlaps \gamma t \implies check-no-overlap \gamma t

unfolding check-no-overlap-alt

proof(induction t)

  case (Cons a t)

  from Cons(1)[OF conjunct1[OF Cons(2)[unfolded no-overlaps.simps]]]

  show \case using conjunct2[OF Cons(2)[unfolded no-overlaps.simps]]

  unfolding check-no-overlap2-def

  by auto

  qed (simp add: check-no-overlap2-def)


lemma (\A e. e \in set t \implies \neg \gamma (ofe-fields e) p) \implies no-overlaps \gamma t

by(induction t) simp-all

lemma no-overlaps-append: no-overlaps \gamma (x \@ y) \implies no-overlaps \gamma y

by(induction x) simp-all

lemma no-overlaps-ne1: no-overlaps \gamma (x \@ a \# y \@ b \# z) \implies ((\exists p. \gamma (ofe-fields a) p) \vee (\exists p. \gamma (ofe-fields b) p)) \implies a \neq b

proof (rule notI, goal-cases contr)

  case contr

  from contr(1) no-overlaps-append have no-overlaps \gamma (a \# y \@ b \# z) by blast

  note this[unfolded no-overlaps.simps]

  with contr(3) have \neg (\exists p \in UNIV. \gamma (ofe-fields a) p \wedge \gamma (ofe-fields b) p) by simp

  with contr(2) show False unfolding contr(3) by simp

  qed


lemma no-overlaps-defeq: no-overlaps \gamma fe \implies OF-same-priority-match2 \gamma fe p = OF-priority-match \gamma fe p

unfolding OF-same-priority-match2-def OF-priority-match-def

unfolding f-Img-ex-set

unfolding prio-match-matcher-alt

unfolding prio-match-matcher-alt2

proof (goal-cases uf)

  case uf

  let \?m' = let m = f \leftarrow fe . \gamma (ofe-fields f) p \in [f \leftarrow m \cdot \forall fo \in set m. ofe-prio fo \leq ofe-prio f]

  let \?s = ofe-action ' set ?m'

  from uf show \case

  proof(cases \?m')

  case Nil

  moreover then have card ?s = 0 by force

  ultimately show \?thesis by(simp add: Let-def)

  next

  case (Cons a as)

  have as = []

  proof(rule contr)

  assume as \neq []

  then obtain b bs where bs: as = b \# bs by (meson neq-Nil-conv)

  note no = Cons[unfolded Let-def filter-filter]

  have f1: a \in set ?m' b \in set ?m' unfolding bs local.Cons by simp-all

  hence ofe-prio a = ofe-prio b by (simp add: antisym)
moreover have ms: γ (ofe-fields a) p γ (ofe-fields b) p using no[symmetric] unfolding bbs by (blast dest: Cons-eq-filterD)+
moreover have abis: a ∈ set fe b ∈ set fe using f1 by auto
moreover have a ≠ b proof (cases ∃ x y z. fe = x @ a # y @ b # z)
  case True
  then obtain x y z where xyz: fe = x @ a # y @ b # z by blast
  from no-overlaps-ne1 ms(1) uf [unfolded xyz]
  show ?thesis by blast
next
  case False
  then obtain x y z where xyz: fe = x @ b # y @ a # z
  using no unfolding bbs by (metis (no-types, lifting) Cons-eq-filterD)
  from no-overlaps-ne1 ms(1) uf [unfolded xyz]
  show ?thesis by blast
  qed
ultimately show False using check-no-overlapI [OF uf, unfolded check-no-overlap-def] by blast
  qed
then have oe: a # as = [a] by simp
  show ?thesis using Cons [unfolded oe] by force
  qed
  qed

lemma distinct fe ⇒ check-no-overlap γ fe ⇒ OF-same-priority-match2 γ fe p = OF-priority-match γ fe p
  by (rule no-overlaps-defeq) (drule (2) no-overlapsI)

theorem OF-eq:
  assumes no: no-overlaps γ f
  and so: sorted-descending (map ofe-prio f)
  shows OF-match-linear γ f p = OF-priority-match γ f p
  unfolding no-overlaps-defeq [symmetric, OF no] OF-match-eq [OF so check-no-overlapI [OF no]]
  ..
corollary OF-eq-sort:
  assumes no: no-overlaps γ f
  shows OF-priority-match γ f p = OF-match-linear γ (sort-descending-key ofe-prio f) p
  using OF-match-eq2 check-no-overlapI no no-overlaps-defeq by fastforce
lemma OF-lm-noa-none: OF-match-linear γ ft p = NoAction ⇒ ∀ e ∈ set ft. ¬ γ (ofe-fields e) p
  by (induction ft) (simp-all split: if-splits)

lemma OF-spm3-noa-none:
  assumes no: no-overlaps γ ft
  shows OF-priority-match γ ft p = NoAction ⇒ ∀ e ∈ set ft. ¬ γ (ofe-fields e) p
  unfolding OF-eq-sort [OF no] by (drule OF-lm-noa-none) simp

lemma no-overlaps-not-undefined: no-overlaps γ ft ⇒ OF-priority-match γ ft p ≠ Undefined
  using check-no-overlapI no-overlaps-not-undefined no-overlaps-defeq by fastforce

end
theory OpenFlow-Serialize
imports OpenFlow-Matches

12
definition serialization-test-entry ≡ OFEntry 7 (EtherDst 0x1, IPv4Dst (PrefixMatch 0xA000201 32), IngressPort "s1 – lan", L4Dst 0x50 0, L4Src 0x3FF, IPv4Proto 6, EtherType 0x800) [ModifyField-l2dst 0xA641F185E862, Forward "s1 – wan"]

definition serialize-mac (m::word) ≡ (intersperse (CHR ".”) o map (hex-string-of-word 1 o (λh. (m >> h * 8) &;& 0xff)) o rev) [0..<6]

lemma serialize-mac 0xdeadbeefcafe = "de:ad:be:ef:ca:fe" by eval

definition serialize-action pids a ≡ (case a of
  ModifyField-l2dst na ⇒ "mod-dl-dst:” @ serialize-mac na)


lemma serialize-actions anything [] = "drop" by(simp add: serialize-actions-def)

definition prefix-to-string pfx ≡ ipv4-cidr-toString (pfxm-prefix pfx, pfxm-length pfx)

primrec serialize-of-match where
serialize-of-match (IngressPort p) = "in-port=" @ pids p |
serialize-of-match (VlanId i) = "dl-vlan=" @ dec-string-of-word0 i |
serialize-of-match (VlanPriority i) = undefined |
serialize-of-match (EtherType i) = "dl-type=0x" @ hex-string-of-word0 i |
serialize-of-match (EtherSrc m) = "dl-src=" @ serialize-mac m |
serialize-of-match (EtherDst m) = "dl-dst=" @ serialize-mac m |
serialize-of-match (IPv4Proto i) = "nw,proto==" @ dec-string-of-word0 i |
serialize-of-match (IPv4Src p) = "nw-src=" @ prefix-to-string p |
serialize-of-match (IPv4Dst p) = "nw-dst=" @ prefix-to-string p |
serialize-of-match (L4Src i m) = "tp-src=" @ dec-string-of-word0 i @ (if m = max-word then [] else "/0x" @ hex-string-of-word3 m) |
serialize-of-match (L4Dst i m) = "tp-dst=" @ dec-string-of-word0 i @ (if m = max-word then [] else "/0x" @ hex-string-of-word3 m)

definition serialize-of-matches :: (string ⇒ string) ⇒ of-match-field set ⇒ string
  where
    serialize-of-matches pids ≡ (λx. "hard-timeout=0,idle-timeout=0," o intersperse (CHR ".”) o map (serialize-of-match pids) o sorted-list-of-set)

lemma serialize-of-matches pids of-matches=
  (List.append "hard-timeout=0,idle-timeout=0,"
(intersperse (CHR ".") (map (serialize-of-match pids) (sorted-list-of-set-of-matches)))
by (simp add: serialize-of-matches-def)

export-code serialize-of-matches checking SML

lemma serialize-of-matches (loif. "42") (ofe-fields serialization-test-entry) =
"hard-timeout=0, idle-timeout=0, in-port=42, dl-type=0x800, dl-dst=00:00:00:00:01, nw-proto=6, nw-dst=10.0.2.1/32, tp-src=1024"
by eval

definition serialize-of-entry pids e \equiv (case e of (OFEntry p f a) \Rightarrow "\text{priority}=" @ dec-string-of-word0 p @ "," @ serialize-of-matches pids f @ "," @ "\text{action}=" @ serialize-actions pids a)

lemma serialize-of-entry (the \circ map-of ["s1-lan","42"],("s1-wan","1337")]) serialization-test-entry =
"\text{priority}=7, hard-timeout=0, idle-timeout=0, in-port=42, dl-type=0x800, dl-dst=00:00:00:00:01, nw-proto=6, nw-dst=10.0.2.1/32, tp-src=1024"
by eval

end

theory Featherweight-OpenFlow-Comparison

imports Semantics-OpenFlow

begin

inductive guha-table-semantics :: ('m, 'p) field-matcher \Rightarrow ('m, 'a) flowtable \Rightarrow 'p \Rightarrow 'a option \Rightarrow bool where

| guha-matched: | ofe-fields fe p = True \Rightarrow
| \forall fe' \in set (ft1 \@ ft2). ofe-prio fe' > ofe-prio fe \Rightarrow \gamma (ofe-fields fe') p = False \Rightarrow
| guha-table-semantics \gamma (ft1 \@ fe \# ft2) p (Some (ofe-action fe)) |
| guha-unmatched: | \forall fe \in set ft. \gamma (ofe-fields fe) p = False \Rightarrow
| guha-table-semantics \gamma ft p None

lemma guha-table-semantics-ex2res:
  assumes ta: CARD('a) \geq 2
  assumes ms: \exists ff. \gamma ff p
  shows \exists ft (a1 :: 'a) (a2 :: 'a). a1 \neq a2 \land guha-table-semantics \gamma ft p (Some a1) \land guha-table-semantics \gamma ft p (Some a2)

proof
  from ms obtain ff where m: \gamma ff p ..
  from ta obtain a1 a2 :: 'a where as: a1 \neq a2 using card2-e1 by blast
  let ?fe1 = OFEntry 0 ff a1
  let ?fe2 = OFEntry 0 ff a2
  let ?ft = [?fe1, ?fe2]
  have guha-table-semantics \gamma ?ft p (Some a1) guha-table-semantics \gamma ?ft p (Some a2)
  by (rule guha-table-semantics.intros(1))[of \gamma ?fe1 p \[ ?fe2 \], unfolded append-Nil flow-entry-match.set] |
    rule guha-table-semantics.intros(1)[of \gamma ?fe2 p \[ ?fe1 \], unfolded append-Nil2 flow-entry-match.set append.simps] |
    simp add: m)+
  thus ?thesis using as by(intro ex1 conjI)
qed

lemma guha-amstaendlich:
  assumes ae: a = ofe-action fe
  assumes ele: fe \in set ft
  assumes rest: \gamma (ofe-fields fe) p
  \forall fe' \in set ft. ofe-prio fe' > ofe-prio fe \Rightarrow \neg \gamma (ofe-fields fe') p
  shows guha-table-semantics \gamma ft p (Some a)
proof –
from ele obtain ft1 ft2 where ftspl: ft = ft1 @ fe # ft2 using split-list by fastforce
show ?thesis unfolding ae ftspl
  apply(rule guha-table-semantics.intro(1))
  using rest(1) apply(simp)
  using rest(2)[unfolded ftspl] apply simp
done
qed

lemma guha-matched-rule-inversion:
assumes guha-table-semantics γ ft p (Some a)
shows ∃fe ∈ set ft. a = ofe-action fe ∧ γ (ofe-fields fe) p ∧ (∀fe′ ∈ set ft. ofe-prio fe′ > ofe-prio fe −→ ¬γ (ofe-fields fe′)) p)
proof –
{ fix d
  assume guha-table-semantics γ ft p d
  hence Some a = d =⇒ (∃fe ∈ set ft. a = ofe-action fe ∧ γ (ofe-fields fe) p ∧ (∀fe′ ∈ set ft. ofe-prio fe′ > ofe-prio fe −→ ¬γ (ofe-fields fe′)) p))
  by (induction rule: guha-table-semantics.induct) simp-all }
from this[OF assms refl] show ?thesis .
qed

lemma guha-equal-Action:
assumes no: no-overlaps γ ft
assumes spm: OF-priority-match γ ft p = Action a
shows guha-table-semantics γ ft p (Some a)
proof –
show ?thesis
  apply(rule guha-umstaendlich)
  apply(rule a[symmetric])
  apply(rule fein)
  using feana unfolding OF-priority-match-ana-def
  apply(auto dest!: filter-singleton split: list.splits)
done
qed

lemma guha-equal-NoAction:
assumes no: no-overlaps γ ft
assumes spm: OF-priority-match γ ft p = NoAction
shows guha-table-semantics γ ft p None
using spm unfolding OF-priority-match-def
by (auto simp add: filter-empty-cone OF-spm3-noa-none[OF no spm] intro: guha-table-semantics.intros(2) split: list.splits)

lemma guha-equal-blp:
assumes no: no-overlaps γ ft
shows guha-table-semantics γ ft p (ftb-to-option (OF-priority-match γ ft p))
unfolding ftb-to-option-def
apply(cases (OF-priority-match γ ft p))
apply(simp add: guha-equal-Action[OF no])
apply(simp add: guha-equal-NoAction(OF no))
apply(subgoal-tac False, simp)
apply(simp add: no no-overlaps-not-unified)
done

lemma guha-deterministic1: guha-table-semantics γ ft p (Some x1) \implies \neg guha-table-semantics γ ft p None

by(auto simp add: guha-table-semantics.simps)

lemma guha-deterministic2: [no-overlaps γ ft; guha-table-semantics γ ft p (Some x1); guha-table-semantics γ ft p (Some a)] \implies x1 = a
proof(rule ccontr, goal-cases)
case 1
note 1(2−3)[THEN guha-matched-rule-inversion]
then obtain fe1 fe2 where fes:
fe1\in\set ft x1 = ofe-action fe1 γ (ofe-fields fe1) p (∀ fe′\in\set ft. ofe-prio fe1 < ofe-prio fe′ \implies \neg γ (ofe-fields fe′) p)
fe2\in\set ft a = ofe-action fe2 γ (ofe-fields fe2) p (∀ fe′\in\set ft. ofe-prio fe2 < ofe-prio fe′ \implies \neg γ (ofe-fields fe′) p)
by blast

from \exists x1 \neq a have fene: fe1 \neq fe2 using fes(2,6) by blast
have pe: ofe-prio fe1 = ofe-prio fe2 using fes(1,3−4,5,7−8) less-linear by blast

note (no-overlaps γ ft)[THEN check-no-overlapI, unfolded check-no-overlap-def]

note this[unfolded Ball-def, THEN spec, THEN spec, THEN mp, OF fes(1), THEN spec, THEN mp, OF fes(5),THEN spec, THEN mp, UNIV-1, OF p] pe fene fes(3,7)
thus False by blast
qed

lemma guha-equal:
assumes no: no-overlaps γ ft
shows OF-priority-match γ ft p = option-to-ftb d \iff guha-table-semantics γ ft p d

using assms
apply(unfold check-no-overlap-def)
apply(clarsimp)
apply(rename-tac fe1 fe2 p)
apply(rule_tac x = fe1 in exI)
apply(simp)
apply(rule_tac x = fe2 in exI)
apply(simp)
apply(rule_tac x = p in exI)
apply(rule conjI)
apply(subst guha-table-semantics.simps)
apply(rule disjI)
done

lemma guha-nondeterministicD:
assumes ¬ check-no-overlap γ ft
shows \exists fe1 fe2 p. fe1 \in \set ft \land fe2 \in \set ft
\land guha-table-semantics γ ft p (Some (ofe-action fe1))
\land guha-table-semantics γ ft p (Some (ofe-action fe2))

using assms
apply(unfold check-no-overlap-def)
apply(clarsimp)
apply(rename-tac fe1 fe2 p)
apply(rule_tac x = fe1 in exI)
apply(simp)
apply(rule_tac x = fe2 in exI)
apply(simp)
apply(rule_tac x = p in exI)
apply(rule conjI)
apply(subst guha-table-semantics.simps)
apply(rule disjI)
apply(clarsimp)
apply(rule-tac x = fe1 in exI)
apply(drule split-list)
apply(clarify)
apply(rename-tac ft1 ft2)
apply(rule-tac x = ft1 in exI)
apply(rule-tac x = ft2 in exI)
apply(simp)
oops

The above lemma does indeed not hold, the reason for this are (possibly partially) shadowed overlaps. This is exemplified below: If there are at least three different possible actions (necessary assumption) and a match expression that matches all packets (convenience assumption), it is possible to construct a flow table that is admonished by check-no-overlap but still will never run into undefined behavior.

lemma
assumes 
CARD(‘action) ≥ 3
assumes ∀ p. γ x p
shows ∃ ft :: (′a, ’action) flow-entry-match list. ¬check-no-overlap γ ft ∧
¬(∃ fe1 fe2 p. fe1 ∈ set ft ∧ fe2 ∈ set ft ∧ fe1 ≠ fe2 ∧ ofe-prio fe1 = ofe-prio fe2 ∧
guha-table-semantics γ ft p (Some (ofe-action fe1)))
∧ guha-table-semantics γ ft p (Some (ofe-action fe2)))
proof −
obtain adef aa ab :: ’action where anb[simp]: aa ≠ ab adef ≠ aa adef ≠ ab using assms(1) card3-eI by blast
let ?cex = [OFEntry 1 x adef, OFEntry 0 x aa, OFEntry 0 x ab]
have ol: ¬check-no-overlap γ ?cex
  unfolding check-no-overlap-def ball-simps
  apply(rule bexl[where x = OFEntry 0 x aa, rotated], (simp;fail))
  apply(rule bexl[where x = OFEntry 0 x ab, rotated], (simp;fail))
  apply(simp add: assms)
done
have df: guha-table-semantics γ ?cex p oc =⇒ oc = Some adef for p oc
unfolding guha-table-semantics.simps
  apply(elim disjE; clarsimp simp: assms)
subgoal for fe ft1 ft2
apply(cases ft1 = [])
apply(fastforce)
apply(cases ft2 = [])
apply(fastforce)
apply(subgoal-tac ft1 = [OFEntry 1 x adef] ∧ fe = OFEntry 0 x aa ∧ ft2 = [OFEntry 0 x ab])
apply(simp;fail)
apply(clarsimp simp add: List.neq-Nil-conv)
apply(rename-tac ya ys yz)
apply(case-tac ys; clarsimp simp add: List.neq-Nil-conv)
done done
show ?thesis
  apply(intro exI[where x = ?cex], intro conjI, fact ol)
  apply(clarify)
  apply(unfold set-simps)
  apply(elim insertE; clarsimp)
  apply((drule df)+; unfold option.inject; (elim anb[symmetric, THEN notE] | (simp;fail))?)+
done
qed
theory LinuxRouter-OpenFlow-Translation
imports IP-Addresses.CIDR-Split
   Automatic-Refinement.Misc
   Simple-Firewall.Generic-SimpleFw
   Semantics-OpenFlow
   OpenFlow-Matches
   OpenFlow-Action
   Routing.Linux-Router
begin
hide-const Misc.uncurry
hide-fact Misc.uncurry-def
definition route2match r =
| iface = ifaceAny, oiface = ifaceAny,
src = (0,0), dst = (pfxm-prefix (routing-match r), pfxm-length (routing-match r)),
proto = ProtoAny, sports = (0,max-word), ports = (0,max-word)|
definition toprefixmatch where
toprefixmatch m ≡ (let pm = PrefixMatch (fst m) (snd m) in if pm = PrefixMatch 0 0 then None else Some pm)
lemma prefix-match-semantics-simple-match:
assumes some: toprefixmatch m = Some pm
assumes vld: valid-prefix pm
shows prefix-match-semantics pm = simple-match-ip m
using some by (cases m)
(clarsimp simp add: toprefixmatch-def ipset-from-cidr-def pfxm-mask-def fun-eq-iff
prefix-match-semantics-ipset-from-netmask[OF vld]
NOT-mask-shifted-lenword[symmetric]
split: if-splits)
definition simple-match-to-of-match-single ::
(32, 'a) simple-match-scheme
⇒ char list option ⇒ protocol ⇒ (16 word × 16 word) option ⇒ (16 word × 16 word) option ⇒ of-match-field set
where
simple-match-to-of-match-single m ifs proto sport dport ≡
uncurry L4Src ' option2set sport ∪ uncurry L4Dst ' option2set dport
∪ IPv4Proto ' (case proto of ProtoAny ⇒ { } | Proto p ⇒ {p}) — protocol is an 8 word option anyway...
∪ IngressPort ' option2set ifs
∪ IPv4Src ' option2set (toprefixmatch (src m)) ∪ IPv4Dst ' option2set (toprefixmatch (dst m))
∪ {EtherType 0x0800}
definition simple-match-to-of-match :: 32 simple-match ⇒ string list ⇒ of-match-field set list list
where
simple-match-to-of-match m ifs ≡ (let
npm = (λp. fst p = 0 ∧ snd p = max-word);
sb = (λp. if npm p then [None] else if fst p ≤ snd p
then map (Some o (Apfx. (pfxm-prefix pfx, NOT (pfxm-mask pfx)))) (wordinterval-CIDR-split-prefixmatch (WordInterval
(fst p) (snd p)) else []))
in [simple-match-to-of-match-single m if proto m) sport dport,
ifs ← (if iface m = ifaceAny then [None] else [Some i. i ← ifs, match-iface (iface m) i]),
sport ← sb (sports m),
dport ← sb (dports m)
)

lemma smtoms-eq-hlp: simple-match-to-of-match-single r a b c d = simple-match-to-of-match-single r f g h i ⟷ (a = f ∧ b = g ∧ c = h ∧ d = i)

proof (rule iffI, goal-cases)
  case 1
  thus ?case proof (intro conjI)
    have *: ∀P z x. [∀x :: of-match-field. P x; z = Some x] ⟹ P (IngressPort x) by simp
    show a = f using 1 by (cases a; cases f)
      (simp add: option2set-None simple-match-to-of-match-single-def toprefixmatch_def option2set-def; subst (asm) set-eq-iff; drule (1) *; simp split: option.splits uncurry-splits protocol.splits) +
  next
    have *: ∀P z x. [∀x :: of-match-field. P x; z = Proto x] ⟹ P (IPv4Proto x) by simp
    show b = g using 1 by (cases b; cases g)
      (simp add: option2set-None simple-match-to-of-match-single-def toprefixmatch_def option2set-def; subst (asm) set-eq-iff; drule (1) *; simp split: option.splits uncurry-splits protocol.splits) +
  next
    have *: ∀P z x. [∀x :: of-match-field. P x; z = Some x] ⟹ P (uncurry L4Src x) by simp
    show c = h using 1 by (cases c; cases h)
      (simp add: option2set-None simple-match-to-of-match-single-def toprefixmatch_def option2set-def; subst (asm) set-eq-iff; drule (1) *; simp split: option.splits uncurry-splits protocol.splits) +
  next
    have *: ∀P z x. [∀x :: of-match-field. P x; z = Some x] ⟹ P (uncurry L4Dst x) by simp
    show d = i using 1 by (cases d; cases i)
      (simp add: option2set-None simple-match-to-of-match-single-def toprefixmatch_def option2set-def; subst (asm) set-eq-iff; drule (1) *; simp split: option.splits uncurry-splits protocol.splits) +
  qed

qed simp

lemma simple-match-to-of-match-generates-prereqs: simple-match-valid m ⟷ r ∈ set (simple-match-to-of-match m ifs) ⟷ all-prerequisites r

unfolding simple-match-to-of-match-def Let-def

proof (clarsimp, goal-cases)
  case (1 xiface xsr p zdstp)
  note o = this
  show ?case unfolding simple-match-to-of-match-single-def all-prerequisites-def
    unfolding ball-un
    proof (intro conjI; (simp fail | −)), goal-cases)
      case 1
      have c: (fst (sports m) = 0 ∧ snd (sports m) = max-word) ∨ proto m = Proto TCP ∨ proto m = Proto UDP ∨ proto m = Proto L4-Protocol.SCTP
        using o(1)
        unfolding simple-match-valid-alt Let-def
        by (clarsimp split: if-splits)
      show ?case
        using o(3) e
        by (elim disjE; simp add: option2set-def split: if-splits prod.splits uncurry-splits)
    next
      case 2
      have c: (fst (dports m) = 0 ∧ snd (dports m) = max-word) ∨ proto m = Proto TCP ∨ proto m = Proto UDP ∨ proto m = Proto L4-Protocol.SCTP

using o(1)

unfolding simple-match-valid-alt Let-def
by(clarsimp split: if-splits)

show ?case
using o(4) e
by(elim disjE; simp add: option2set-def split: if-splits prod.splits uncurry-splits)

qed

lemma and-assoc: a ∧ b ∧ c ↔ (a ∧ b) ∧ c by simp

lemmas custom-simpset = Let-def set-concat set-map map-map comp-def concat-map-maps set-maps UN-iff fun-app-def Set.image-iff

abbreviation simple-fw-prefix-to-wordinterval ≡ prefix-to-wordinterval ◦ uncurry PrefixMatch

lemma simple-match-port-alt: simple-match-port m p ↔ p ∈ wordinterval-to-set (uncurry WordInterval m) by(simp split: uncurry-splits)

lemma simple-match-src-alt: simple-match-valid r ⇒ simple-match-ip (src r) p ↔ prefix-match-semantics (PrefixMatch (fst (src r)) (snd (src r))) p by(cases (src r)) (simp add: prefix-match-semantics-ipset-from-netmask2 prefix-to-wordset-ipset-from-cidr simple-match-valid-def valid-prefix-fw-def)

lemma simple-match-dst-alt: simple-match-valid r ⇒ simple-match-ip (dst r) p ↔ prefix-match-semantics (PrefixMatch (fst (dst r)) (snd (dst r))) p by(cases (dst r)) (simp add: prefix-match-semantics-ipset-from-netmask2 prefix-to-wordset-ipset-from-cidr simple-match-valid-def valid-prefix-fw-def)

lemma x ∈ set (wordinterval-CIDR-split-prefixmatch w) ⇒ valid-prefix x using wordinterval-CIDR-split-prefixmatch-all-valid-Ball[THEN bspec, THEN conjunct1].

lemma simple-match-to-of-matchI:
assumes mv: simple-match-valid r
assumes mm: simple-matches r p
assumes ii: p-iiface p ∈ set ifs
assumes ipkt: p-l2type p = 0x800
shows eq: ∃ gr ∈ set (simple-match-to-of-match r ifs). OF-match-fields gr p = Some True

definition pnm ≡ λ p. fst p = 0 ∧ snd p = max-word

lemma simple-match-to-of-match1:
assumes ?npm: p-l2type p = 0x800
shows eq: ∃ gr ∈ set (simple-match-to-of-match r ifs). OF-match-fields gr p = Some True

proof —
let ?sb = λ r. (if ?npm p then None else Some r)

obtain si where si: case si of Some ssi ⇒ p-sport p ∈ prefix-to-wordset ssi | None ⇒ True
case si of None ⇒ True | Some ssi ⇒ ssi ∈ set (wordinterval-CIDR-split-prefixmatch (uncurry WordInterval (sports r))))

proofcases ?npm (sports r), goal-cases

case 1
hence (case None of None ⇒ True | Some ssi ⇒ p-sport p ∈ prefix-to-wordset ssi) ∧
(case None of None ⇒ True
 | Some ssi ⇒ ssi ∈ set (wordinterval-CIDR-split-prefixmatch (uncurry WordInterval (sports r)))) by simp

with 1 show ?thesis by blast
next
case 2
from mm have p-sport p ∈ wordinterval-to-set (uncurry WordInterval (sports r)) by(simp only: simple-matches.simps simple-match-port-alt)
then obtain $ssi$ where $ssi$:

$sni \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ (\text{uncurry WordInterval} \ (\text{sports} \ r)))$

$p$-sport $p \in \text{prefix-to-wordset} \ ssi$

using $\text{wordinterval-CIDR-split-existential}$ by fast

hence (case $\text{Some} \ ssi \equiv \text{None} \Rightarrow \text{True}$ | $\text{Some} \ ssi \Rightarrow p$-sport $p \in \text{prefix-to-wordset} \ ssi$) \land

(case $\text{Some} \ ssi \equiv \text{None} \Rightarrow \text{True}$ | $\text{Some} \ ssi \Rightarrow ssi \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ (\text{uncurry WordInterval} \ (\text{sports} \ r)))$) by simp

with 2 show $\text{thesis}$ by blast

qed

obtain $di$ where $di$: case $di$ of $\text{None} \Rightarrow p$-port $p \in \text{prefix-to-wordset} \ ddi$ | $\text{None} \Rightarrow \text{True}$

case $\text{di}$ of $\text{None} \Rightarrow \text{True}$ | Some $ddi \Rightarrow ddi \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ (\text{uncurry WordInterval} \ (\text{dports} \ r)))$

di = $\text{None} \iff ?npm \ (\text{dports} \ r)$

proof
(cases $?npm \ (\text{dports} \ r)$, goal-cases)

case 1

hence (case $\text{None} \equiv \text{None} \Rightarrow \text{True}$ | $\text{Some} \ ssi \Rightarrow p$-port $p \in \text{prefix-to-wordset} \ ssi$) \land

(case $\text{None} \equiv \text{None} \Rightarrow \text{True}$ | $\text{Some} \ ssi \Rightarrow ssi \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ (\text{uncurry WordInterval} \ (\text{dports} \ r)))$) by simp

with 1 show $\text{thesis}$ by blast

next

case 2

from $mm$ have $p$-port $p \in \text{wordinterval-to-set} \ (\text{uncurry WordInterval} \ (\text{dports} \ r))$

by (simp only: simple-matches.simps simple-match-port-alt)

then obtain $ddi$ where $ddi$:

$ddi \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ (\text{uncurry WordInterval} \ (\text{dports} \ r)))$

$p$-port $p \in \text{prefix-to-wordset} \ ddi$

using $\text{wordinterval-CIDR-split-existential}$ by fast

hence (case $\text{Some} \ ddi \equiv \text{None} \Rightarrow \text{True}$ | $\text{Some} \ ssi \Rightarrow p$-port $p \in \text{prefix-to-wordset} \ ssi$) \land

(case $\text{Some} \ ddi \equiv \text{None} \Rightarrow \text{True}$ | $\text{Some} \ ssi \Rightarrow ssi \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ (\text{uncurry WordInterval} \ (\text{dports} \ r)))$) by simp

with 2 show $\text{thesis}$ by blast

qed

let $?mf = \text{map-option} \ (\text{apsnd} \ (\text{wordNOT} \ o \ \text{mask} \ o \ (-) \ 16) \ o \ \text{prefix-match-dtor})$

let $?gr = \text{simple-match-to-of-match-single} \ r$

(if $\text{iiface} \ r \equiv \text{iFaceAny} \text{then None else Some} \ (\text{p-iiface} \ p)$)

(if $\text{proto} \ r \equiv \text{ProtoAny} \text{then ProtoAny else Proto} \ (\text{p-proto} \ p)$)

($?mf \ ssi$) ($?mf \ di$

note $\text{mfu} = \text{simple-match-port.simps[of \ fst \ (\text{sports} \ r) \ \text{snd} \ (\text{sports} \ r), \ unfolded \ surjective-pairing[\text{of \ \text{sports} r, symmetric]]}$

\text{simple-match-port.simps[of \ fst \ (\text{dports} \ r) \ \text{snd} \ (\text{dports} \ r), \ unfolded \ surjective-pairing[\text{of \ \text{dports} r, symmetric]]}$

note $u = mm[\text{unfolded \ simple-matches.simps \ mfu \ ord-class.atLeastAtMost-iff \ simple-packet-unext-def \ simple-packet.simps]}$

\text{note \ \text{of-safe-unsafe-match-eq[OF \ \text{simple-match-to-of-match-generates-preq}]}$

from $u$ have $\text{ple: \ fst} \ (\text{sports} \ r) \ \leq \ \text{snd} \ (\text{sports} \ r) \ \text{fst} \ (\text{dports} \ r) \ \leq \ \text{snd} \ (\text{dports} \ r)$ by force+

show $\text{eg.:} \ ?gr \in \text{set} \ (\text{simple-match-to-of-match \ r \ \text{ifs}})$

unfolding $\text{simple-match-to-of-match-def}$

unfolding custom-simpset

unfolding sntoms-eq-hlp

proof
(intro bexI, (intro conjl; ((rule refl) ?)), goal-cases)

case 2 thus $\text{case using \ ple(2) \ di}$

apply (simp add: pfmt-mask-def prefix-match-dtor-def Set.image-iff

split: option.splits prod.splits uncurry-splits)

apply (erule bexI[rotated])

apply (simp split: prefix-match_splits)

21
done

next

case 3 thus ?case using ple(1) si
  apply(simp add: pfzm-mask-def prefix-match-dtor-def Set.image-iff
     split: option.splits prod.splits uncurry.splits)
  apply(erule bexI[rotated])
  apply(simp split: prefix-match.splits)
done

next

case 4 thus ?case
  using u ii by(clarsimp simp: set-maps split: if-splits)

next

case 1 thus ?case using ii u by simp-all (metis match,proto.elims(2))
qed

have dpm: \( \text{di} = \text{Some} \ (\text{PrefixMatch} \ x1 \ x2) \Rightarrow p-dport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \text{ for } x1 \ x2 \)
proof –
  have \( \ast: \text{di} = \text{Some} \ (\text{PrefixMatch} \ x1 \ x2) \Rightarrow \text{prefix-match-semantics} \ (\text{the } \text{di}) \ (p-dport \ p) \Rightarrow p-dport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \)
  by(clarsimp simp: prefix-match-semantics-def pfzm-mask-def word-bw-comms;fail)
  have \( \ast\ast: \text{pfz} \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ \text{ra}) \Rightarrow \text{prefix-match-semantics} \ \text{pfz} \ a = (a \in \text{prefix-to-wordset} \ \text{pfz}) \)
  for \( \text{pfz} \ \text{ra} \text{ and } a::16 \text{ word} \)
  by \( \text{fact prefix-match-semantics-wordset(OF wordinterval-CIDR-split-prefixmatch-all-valid-Ball[THEN bspec, THEN conjunct1])} \)
  have \[ di = Some (PrefixMatch x1 x2); p-dport p \in prefix-to-wordset (PrefixMatch x1 x2); PrefixMatch x1 x2 \in set (wordinterval-CIDR-split-prefixmatch (uncurry WordInterval (dports r)))\]
  \( \Rightarrow p-dport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \)
  using di(1,2)
  using \( \ast\ast \text{ by auto} \)
  thus \( \text{di} = \text{Some} \ (\text{PrefixMatch} \ x1 \ x2) \Rightarrow p-dport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \text{ using } \text{di}(1,2) \text{ by auto} \)
qed

have spm: \( \text{si} = \text{Some} \ (\text{PrefixMatch} \ x1 \ x2) \Rightarrow p-sport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \text{ for } x1 \ x2 \)
using si
proof –
  have \( \ast: \text{si} = \text{Some} \ (\text{PrefixMatch} \ x1 \ x2) \Rightarrow \text{prefix-match-semantics} \ (\text{the } \text{si}) \ (p-sport \ p) \Rightarrow p-sport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \)
  by(clarsimp simp: prefix-match-semantics-def pfzm-mask-def word-bw-comms;fail)
  have \( \ast\ast: \text{pfz} \in \text{set} \ (\text{wordinterval-CIDR-split-prefixmatch} \ \text{ra}) \Rightarrow \text{prefix-match-semantics} \ \text{pfz} \ a = (a \in \text{prefix-to-wordset} \ \text{pfz}) \)
  for \( \text{pfz} \ \text{ra} \text{ and } a::16 \text{ word} \)
  by \( \text{fact prefix-match-semantics-wordset(OF wordinterval-CIDR-split-prefixmatch-all-valid-Ball[THEN bspec, THEN conjunct1])} \)
  have \[ si = Some (PrefixMatch x1 x2); p-sport p \in prefix-to-wordset (PrefixMatch x1 x2); PrefixMatch x1 x2 \in set (wordinterval-CIDR-split-prefixmatch (uncurry WordInterval (dports r)))\]
  \( \Rightarrow p-sport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \)
  using si(1,2)
  using \( \ast\ast \text{ by auto} \)
  thus \( \text{si} = \text{Some} \ (\text{PrefixMatch} \ x1 \ x2) \Rightarrow p-sport \ p \ \&\& \sim\sim \ (\text{mask} \ (16 - x2)) = x1 \text{ using } \text{si}(1,2) \text{ by auto} \)
qed

show OF-match-fields \( ?gr \ p = \text{Some} \ \text{True} \)

unfolding of-safe-unsafe-match-eq[OF simple-match-to-of-match-generates-prereqs[OF mv eg]]
by(cases si; cases di)
(simp-all
  add: simple-match-to-of-match-single-def OF-match-fields-unsafe-def spm
  option2set-def u ipplt prefix-match-dtor-def toprefixmatch-def dpm
  simple-match-dst-alt[OF mv, symmetric] simple-match-src-alt[OF mv, symmetric]
split: prefix-match.splits

qed

lemma prefix-match-00[simp.intro]: prefix-match-semantics (PrefixMatch 0 0) p
by (simp add: valid-prefix-def zero-prefix-match-all)

lemma simple-match-to-of-matchD:
assumes eg: gr ∈ set (simple-match-to-of-match r ifs)
assumes mo: OF-match-fields gr p = Some True
assumes me: match-iface (oface r) (p-oface p)
assumes mv: simple-match-valid r
shows simple-matches r p
proof –
from mv have validpfx:
  \(\forall pm.\) toprefmtopmatch (src r) = Some pm \(\Rightarrow\) valid-prefix pm
  \(\forall pm.\) toprefmtopmatch (dst r) = Some pm \(\Rightarrow\) valid-prefix pm
unfolding simple-match-valid-def valid-prefix-fu-def toprefmtopmatch-def
by (simp-all split: uncurry-splits if-splits)
from mo have mo: OF-match-fields-unsafe gr p
unfolding of-safe-unsafe-match-eq [OF simple-match-to-of-match-generates-prereqs [OF mv eg]]
by simp
note this[unfolded OF-match-fields-unsafe-def]
note eg[unfolded simple-match-to-of-match-def simple-match-to-of-match-single-def custom-simpset option2set-def]
then guess x .. moreover from this(2) guess xa .. moreover from this(2) guess xb ..
note xx = calculation(1,3) this

{ fix a b xc xa
  fix pp :: 16 word
  have [pp && ~ (pfxm-mask xc) = pfxm-prefix xc] \(\Rightarrow\) prefix-match-semantics xc (pp) for xc
      by (simp add: prefix-match-semantics-def word-bw-comms:fail)
    moreover have pp ∈ wordinterval-to-set (WordInterval a b) \(\Rightarrow\) a ≤ pp ∧ pp ≤ b by simp
    moreover have xc ∈ set (wordinterval-CIDR-split-prefixmatch (WordInterval a b)) \(\Rightarrow\) pp ∈ prefix-to-wordset xc \(\Rightarrow\) pp ∈ wordinterval-to-set (WordInterval a b)
      by (subt wordinterval-CIDR-split-prefixmatch) blast
    moreover have [xc ∈ set (wordinterval-CIDR-split-prefixmatch (WordInterval a b)); xa = Some (pfxm-prefix xc, ~ (pfxm-mask xc)); prefix-match-semantics xc (pp)] \(\Rightarrow\) pp ∈ prefix-to-wordset xc
      apply (subst (asm) (1) prefix-match-semantics-wordset)
      apply (erule wordinterval-CIDR-split-prefixmatch-all-valid-Ball[THEN bspec, THEN conjunct1]; fail)
      apply assumption
    done
  ultimately have [xc ∈ set (wordinterval-CIDR-split-prefixmatch (WordInterval a b)); xa = Some (pfxm-prefix xc, ~ (pfxm-mask xc)); pp && ~ (pfxm-mask xc) = pfxm-prefix xc] \(\Rightarrow\) a ≤ pp ∧ pp ≤ b
    by metis
} note l4port-logic = this

show ?thesis unfolding simple-matches.simps
proof(unfold and-assoc, (rule)+)
  show match-iface (iiface r) (p-iiface p)
  apply(cases iiface r = ifaceAny)
apply (simp add: match-ifaceAny)
using xx(1) mo unfolding xx(4) OF-match-fields-unsafe-def
apply(simp only: if-False set-maps UN-iff)
apply(clarify)
apply(rename-tac a; subgoal-tac match-iface (iface r) a)
apply(clarsimp simp add: option2set-def fail)
apply(rule ccontr, simp; fail)
done
next
show match-iface (oiface r) (p-oiface p) using me .
next
show simple-match-ip (src r) (p-src p)
using mo unfolding xx(4) OF-match-fields-unsafe-def toprefixmatch-def
by(clarsimp simp add: simple-packet-unext-def prefix-match-semantics-simple-match ball-Un
split: if-splits)
next
show simple-match-ip (dst r) (p-dst p)
using mo unfolding xx(4) OF-match-fields-unsafe-def toprefixmatch-def
by(clarsimp simp add: simple-packet-unext-def prefix-match-semantics-simple-match ball-Un
split: if-splits)
next
show match-proto (proto r) (p,proto p)
using mo unfolding xx(4) OF-match-fields-unsafe-def
using xx(1) by(clarsimp simp add: prefix-match-semantics-simple-match ball-Un
split: protocol.splits)
next
show simple-match-port (sports r) (p-sport p)
using mo xx(2) unfolding xx(4) OF-match-fields-unsafe-def
by(cases sports r) (clarsimp simp add: l4port-logic prefix-match-semantics-simple-match split: if-splits)
next
show simple-match-port (dports r) (p-dport p)
using mo xx(3) unfolding xx(4) OF-match-fields-unsafe-def
by(cases dports r) (clarsimp simp add: l4port-logic prefix-match-semantics-simple-match split: if-splits)
qed

primrec annotate-rlen where
annotate-rlen [] = [] |
annotate-rlen (a#as) = (length as, a) # annotate-rlen as

lemma annotate-rlen "asdf" = [3, CHR "a"], (2, CHR "s"), (1, CHR "d"), (0, CHR "f") by simp

lemma fst-annotate-rlen-le: (k, a) ∈ set (annotate-rlen l) ⇒ k < length l
by(induction l arbitrary: k; simp; force)

lemma distinct-fst-annotate-rlen: distinct (map fst (annotate-rlen l))
using fst-annotate-rlen-le by(induction l) (simp, fastforce)

lemma distinct-annotate-rlen: distinct (annotate-rlen l)
using distinct-fst-annotate-rlen unfolding distinct-map by blast

lemma in-annotate-rlen: (a,x) ∈ set (annotate-rlen l) ⇒ x ∈ set l
by (induction l) (simp-all, blast)

lemma map snd annotate-rlen: map snd (annotate-rlen l) = l
  by (induction l) simp-all

lemma sorted-descending (map fst (annotate-rlen l))
  by (induction l; clarsimp) (force dest: fst-annotate-rlen-le)

lemma annotate-rlen l = zip (rev [0..<length l]) l
  by (induction l; simp)

primrec annotate-rlen-code where
annotate-rlen-code [] = ()
annotate-rlen-code (a # as) = (case annotate-rlen-code as of (r, as) => (Suc r, (r, a) # as))

lemma annotate-rlen-len: fst (annotate-rlen-code r) = length r
  by (induction r) (clarsimp split: prod.splits)+

lemma annotate-rlen-code [code]: annotate-rlen s = snd (annotate-rlen-code s)
  proof (induction s)
    case (Cons s ss) thus ?case using annotate-rlen-len[of ss] by (clarsimp split: prod.split)
  qed simp

lemma suc2plus-inj-on: inj-on (of-nat :: nat => ('l :: len) word) {0..unat (max-word :: 'l word)}
  proof (rule inj-on)
    let ?mmw = (max-word :: 'l word)
    let ?mstp = (of-nat :: nat => 'l word)
    fix x y :: nat
    assume x \in\ {0..unat ?mmw} y \in {0..unat ?mmw}
    hence se: x \leq unat ?mmw y \leq unat ?mmw by simp-all
    assume eq: ?mstp x = ?mstp y
    note f = le-unat-uoi[OF se(1)] le-unat-uoi[OF se(2)]
    show x = y using eq le-unat-uoi se by metis
  qed

lemma distinct-of-nat-list:
distinct l \implies\ \forall e \in set l. e \leq unat (max-word :: ('l::len) word) \implies distict (map (of-nat :: nat => 'l word) l)
  proof (induction l)
    let ?mmw = (max-word :: 'l word)
    let ?mstp = (of-nat :: nat => 'l word)
    case (Cons a as)
    have distinct as \forall e \in as. e \leq unat ?mmw using Cons.prems by simp-all
    note mIH = Cons.IH[OF this]
    moreover have ?mstp a \notin ?mstp ' set as
      proof
        have representable-set: set as \subseteq\ {0..unat ?mmw} using \forall e \in set (a # as). e \leq unat max-word by fastforce
        have a-reprbl: a \in {0..unat ?mmw} using \forall e \in set (a # as). e \leq unat max-word by simp
        assume ?mstp a \notin ?mstp ' set as
        with inj-on-image-mem-iff[OF suc2plus-inj-on a-reprbl representable-set]
        have a \in set as by simp
        with distinct (a # as) show False by simp
      qed
      ultimately show ?case by simp
  qed simp

lemma annotate-first-le-hlp:
length l < unat (max-word :: ('l :: len) word) \implies\ \forall e \in set (map fst (annotate-rlen l)). e \leq unat (max-word :: 'l word)
  by (clarsimp) (meson fst-annotate-rlen-le less_trans nat-less-le)

lemmas distinct-of-prio-hlp = distinct-of-nat-list[OF distinct-fst-annotate-rlen annotate-first-le-hlp]
lemma `fst-annotate-rlen`: \( \text{map } \text{fst} \ (\text{annotate-rlen } l) = \text{rev } [0..<\text{length } l] \)
by (induction \( l \)) (simp-all)

lemma `sorted-word-upt`:

defines [simp]: \( \text{won } \equiv \ (\text{of-nat } :: \ \text{nat } \Rightarrow \ ('l :: \ \text{len}) \ \text{word}) \)
assumes \( \text{length } l \leq \text{unat } (\text{max-word } :: \ 'l \ \text{word}) \)
shows \( \text{sorted-descending } (\text{map } \text{won} (\text{rev } [0..<\text{Suc } (\text{length } l)])) \)
using \( \text{assms} \)
by (induction \( l \) rule: rev-induct; clarsimp)

(metis (mono-tags, hide-lams) le-SucI le-unat-uoi of-nat-Suc order-refl word-le-nat-alt)

lemma `sorted-annotated`:

assumes \( \text{length } l \leq \text{unat } (\text{max-word } :: (\'l :: \ \text{len}) \ \text{word}) \)
shows \( \text{sorted-descending } (\text{map } \text{fst} (\text{map } (\text{apfst } (\text{of-nat } :: \ \text{nat} ) \Rightarrow \ ('l :: \ \text{len}) \ \text{word}) \ (\text{annotate-rlen } l))) \)
proof
let \( ?\text{won } = (\text{of-nat } :: \ \text{nat} ) \Rightarrow (\'l :: \ \text{len}) \ \text{word} \)

have \( \text{sorted-descending } (\text{map } ?\text{won} (\text{rev } [0..<\text{Suc } (\text{length } l)])) \)
using \( \text{sorted-word-upt} \ [\ \text{OF assms} ] . \)

hence \( \text{sorted-descending } (\text{map } ?\text{won} (\text{map } \text{fst} (\text{map } \text{annotate-rlen } l)))) \)
by (simp add: `fst-annotate-rlen`)

thus \( \text{sorted-descending } (\text{map } \text{fst} (\text{map } (\text{apfst } ?\text{won}) (\text{annotate-rlen } l)))) \)
by simp
qed

l3 device to l2 forwarding

definition `lr-of-tran-s3` ifs ard = ( \( [(p, b, \ \text{case } a \ \text{of simple-action}. \ \text{Accept } \Rightarrow [\ \text{Forward } c \ | \ \text{simple-action}. \ \text{Drop } \Rightarrow []). \]
(p,r,⟨ε,a⟩) ← ard, b ← \text{simple-match-to-of-match } r \ \text{ifs} )\)

definition `oif-ne-iif-p1` ifs = \( [[\text{simple-match-any} (\\text{oiface} := \text{Iface oif}, \ \text{iiface} := \text{Iface iif}), \ \text{simple-action}. \ \text{Accept}). \ \text{oif } ← \ \text{ifs}, \ \text{iif } ← \ \text{ifs}, \ \text{oif } ≠ \ \text{iif}]]\)

definition `oif-ne-iif-p2` ifs = \( [[\text{simple-match-any} (\\text{oiface} := \text{Iface i}, \ \text{iiface} := \text{Iface i}), \ \text{simple-action}. \ \text{Drop}). \ \text{i } ← \ \text{ifs}]]\)

definition `oif-ne-iif` ifs = `oif-ne-iif-p2` ifs @ `oif-ne-iif-p1` ifs

definition `lr-of-tran-s4` ard ifs = `generalized-fw-join` ard (\( \text{oif-ne-iif } \text{ifs} )\)

definition `lr-of-tran-s1` rt = \( [(\text{route2match } r, \ \text{output-iface} (\text{routing-action } r)), \ r ← rt] \)

definition `lr-of-tran-fbs` rt fw ifs = \( \text{let} \)
gfw = \( \text{map } \text{simple-rule-dtor } \text{fw} \); \( \text{— generalized simple fw, hopefully for FORWARD}\)
frt = `lr-of-tran-s1` rt; \( \text{— rt as fw}\)
prd = `generalized-fw-join` frt gfw
\( \text{in } \text{prd} \)

definition `pack-OF-entries` ifs ard = \( \text{map } (\text{split3 } \text{OFEntry} ) \ (\text{lr-of-tran-s3 } \text{ifs } \text{ard} )\)

definition `no-oif-match` ≡ `list-all` (\( \text{λm}. \ \text{ofiface} (\text{match-sel } m ) = \text{ifaceAny} )\)

definition `lr-of-tran rt fw ifs` ≡ \( \text{if } \neg (\text{no-oif-match } \text{fw} \ \text{∧ has-default-policy } \text{fw} \ \text{∧ simple-fw-valid } \text{fw} \ \text{∧ valid-prefixes } \text{rt} \ \text{∧ has-default-route } \text{rt} \ \text{∧ distinct } \text{ifs} ) \)
then Inl "\text{Error in creating OpenFlow table: prerequisites not satisfied}" 
else (
let nrd = lr-of-tran-fbs rt fw ifs;
ard = map (apfst of-nat) (annotate-rlen nrd) — give them a priority
in
if length nrd < unat (max-word :: 16 word)
then Inr (pack-OF-entries ifs ard)
else Inl "Error in creating OpenFlow table: priority number space exhausted"

definition is-iface-name i ≡ i ≠ [] ∧ ~iface.iface-name-is-wildcard i
definition is-iface-list ifs ≡ distinct ifs ∧ list-all is-iface-name ifs

lemma max-16-word-max[simp]: (a :: 16 word) ≤ 0xffff
proof
  have ffff: 0xffff = word-of-int (2 ^ 16 - 1) by fastforce
  show thesis using max-word-max[of a] unfolding max-word-def ffff by fastforce
qed

lemma replicate-FT-hlp: x ≤ 16 ∧ y ≤ 16 ⇒ replicate (16 - x) False @ replicate x True = replicate (16 - y) False @ replicate y True ⇒ x = y
proof
  let ?ns = {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16}
  assume x ≤ 16 ∧ y ≤ 16
  hence x ∈ ?ns by (simp; presburger)+
  moreover assume replicate (16 - x) False @ replicate x True = replicate (16 - y) False @ replicate y True
  ultimately show x = y by simp (elim disjE; simp-all)
qed

lemma mask-inj-hlp1: inj-on (mask :: nat ⇒ 16 word) {0..16}
proof(intro inj-onI, goal-cases)
case (1 x y)
  from 1(3)
  have oe: of-bl (replicate (16 - x) False @ replicate x True) = (of-bl (replicate (16 - y) False @ replicate y True) :: 16 word)
    unfolding mask-bl of-bl-rep-False .
  have f z: z ≤ 16 ⇒ length (replicate (16 - z) False @ replicate z True) = 16 by auto
    with f(1,2)
  have ps: replicate (16 - x) False @ replicate x True ∈ {bl. length bl = LENGTH(16)} replicate (16 - y) False @ replicate y True ∈ {bl. length bl = LENGTH(16)} by simp-all
    from inj-onD(OF word-bl.Abs-inj-on, OF oe ps)
    show ?case using 1(1,2) by (fastforce intro: replicate-FT-hlp)
qed

lemma distinct-simple-match-to-of-match-portlist-hlp:
fixes ps :: (16 word × 16 word)
shows distinct ifs =⇒ distinct
  (if fst ps = 0 ∧ snd ps = max-word then [None]
   else if fst ps ≤ snd ps
     then map (Some o (λpfx. (pfxm-prefix pfx, ~ (pfxm-mask pfx))))
       (wordinterval-CIDR-split-prefixmatch (WordInterval (fst ps) (snd ps)))
     else [])
proof
  assume di: distinct ifs
  { define wis where wis = set (wordinterval-CIDR-split-prefixmatch (WordInterval (fst ps) (snd ps)))}
fix \(x\ y\ ::\ 16\ \text{prefix-match}\)

obtain \(zm\ zm\ ym\ yn\ \text{where}\ \text{zyd [simp]}:\ x = \text{PrefixMatch} zm\ zm\ y = \text{PrefixMatch} ym\ yn\ \text{by} (\text{cases}\ x;\ \text{cases}\ y)\)

assume \(iw\ \text{where} e:\ (\text{pizm-prefix}\ x,\ \ddot{\text{~~}}\ (\text{pizm-mask}\ x)) = (\text{pizm-prefix}\ y,\ \ddot{\text{~~}}\ (\text{pizm-mask}\ y))\)

hence \(le16: x\ \le\ 16\ \text{ym}\ \le\ 16\ \text{unfolding}\ \text{wis-def}\ \text{using}\ \text{wordinterval-CIDR-split-prefixmatch-all-valid-Ball[unfolded Ball-def, THEN spec, THEN mp]}\ \text{by}\ \text{force}\)

with \(et\ \text{have} 16 - zm = 16 - ym\ \text{unfolding}\ \text{pizm-mask-def}\ \text{by} (\text{auto intrd: mask-inj-hlp1 [THEN inj-onD]})\)

hence \(x = y\ \text{using} et\le16\ \text{using}\ \text{diff-diff-cancel}\ \text{by}\ \text{simp}\)

\{\ * = this\}

show \text{thesis}

apply (clarsimp simp add: smtomseq-hlp distinct-map wordinterval-CIDR-split-distinct)
apply (subst comp-inj-on-iff [symmetric]; intro inj-onI)
using \(*\) by simp-all

qed

lemma distinct-simple-match-to-of-match: distinct ifs \(\Rightarrow\) distinct (simple-match-to-of-match m ifs)
apply (unfold simple-match-to-of-match-def Let-def)
apply (rule distinct-3comprI)
subgoal by (induction ifs; clarsimp)
subgoal by (fact distinct-simple-match-to-of-match-portlist-hlp)
subgoal by (fact distinct-simple-match-to-of-match-portlist-hlp)
subgoal by (simp-all add: smtomseq-hlp)
done

lemma inj-inj-on: inj \(F\ \Rightarrow\) inj-on \(F\ A\ \text{using}\ \text{subset-inj-on}\ \text{by}\ \text{auto}\)

lemma no-overlaps-lroft-hlp2: distinct (map \(\text{fst}\ amr\)) \(\Rightarrow\) \((\dot{x}.\ \text{distinct}\ (\text{fn}\ r))\) \(\Rightarrow\)
distinct (concat (map (\(\lambda x. (p,\ r,\ c,\ a)\)). map (\(\lambda y. (p,\ b,\ f,\ a,\ c)\)). (\text{fn}\ r)). amr))
by (induction amr; force intro: injI inj-onI simp add: distinct-map split: prod.splits)

lemma distinct-lroft-s3: [distinct (map \(\text{fst}\ amr))]; distinct ifs \(\Rightarrow\) distinct (lr-of-trans-s3 ifs amr)

unfolding lr-of-trans-s3-def
by (erule no-overlaps-lroft-hlp2, simp add: distinct-simple-match-to-of-match)

lemma no-overlaps-lroft-hlp3: distinct (map \(\text{fst}\ amr)) \(\Rightarrow\)
\((aa,\ ab,\ ac)\in\set (lr-of-trans-s3 ifs amr)\ \Rightarrow\) \((ba,\ bb,\ bc)\in\set (lr-of-trans-s3 ifs amr)\ \Rightarrow\)
\(ac\neq bc\ \Rightarrow\) \(aa\neq ba\)
apply (unfold lr-of-trans-s3-def)
apply (clarsimp)
apply (clarsimp split: simple-action.splits)
apply (metis map-of-eq-Some-iff old.prod.inject option.inject)
apply (metis map-of-eq-Some-iff old.prod.inject option.inject simple-action.distinct (2))
done

lemma no-overlaps-lroft-s3-hlp-hlp:
[distinct (map \(\text{fst}\ amr))]; \(OF\text{-match-fields-unsafe}\ ab\ p;\ ab\neq ad\ \vee\ ba\neq bb;\ \text{OF\text{-match-fields-unsafe}\ ad}\ p;\)
\((ac,\ ab, ba)\in\set (lr-of-trans-s3 ifs amr); (ac, ad, bb)\in\set (lr-of-trans-s3 ifs amr)]\]
\(\Rightarrow\) \text{False}
proof (elim disjE, goal-cases)

case \(I\)

have \(i: [\text{distinct (map \(\text{fst}\ amr))}; (ac, ab, x1, x2)\in\set amr; (ac, bb, x4, x5)\in\set amr; ab\neq bb] \Rightarrow \text{False for} ab x1 x2 bb x4 x5\)
by (meson distinct-map-fstD old.prod.inject)

have conjunctSomeProtoAnyD: Some ProtoAny = simple-proto-conjunct a (Proto b) \(\Rightarrow\) \text{False for} a b
using conjunctProtoD by force

28
have 5:

\[ OF\text{-match-fields-unsafe} \ am \ p; \ OF\text{-match-fields-unsafe} \ bm \ p; \ am \neq \ bm; \\
\ am \in \text{set (simple-match-to-of-match} \ ab \ ifs); \ bm \in \text{set (simple-match-to-of-match} \ bb \ ifs); \ \neg ab \neq bb \] 

\implies False \ for \ ab \ am \ bm

by (clarify | unfold

simple-match-to-of-match-def

smtoms-eq-hlp

Let-def

set-concat

set-map

de-Morgan-conj

not-False-eq-True)+

(auto dest: conjunctSomeProtoAnyD cidrsplit-no-overlaps

simp add: OF-match-fields-unsafe-def

simple-match-to-of-match-single-def

option2set-def

comp-def

split: if-splits

cong: smtoms-eq-hlp)

from 1 show \#case

using 4 5 by (clarsimp simp add: lr-of-tran-s3-def) blast

qed


lemma no-overlaps-lroft-s3-hlp: distinct (map fst amr) \implies distinct ifs \implies

no-overlaps \ OF-match-fields-unsafe (map (split3 OFEntry) (lr-of-tran-s3 ifs amr))

apply (rule no-overlapsI [rotated])

apply (subt distinct-map, rule conjI)

subgoal by (erule (1) distinct-lroft-s3)

subgoal

apply (rule inj-inj-on)

apply (rule injI)

apply (rename-tac x y, case-tac x, case-tac y)

apply (simp add: split3-def fail)

done

subgoal

apply (unfold check-no-overlap-def)

apply (clarify)

apply (unfold set-map)

apply (clarify)

apply (unfold split3-def prod.simps flow-entry-match.simps flow-entry-match.sel de-Morgan-conj)

apply (clarsimp simp: simps)

apply (erule (1) no-overlaps-lroft-s3-hlp-hlp)

apply simp

apply assumption

apply assumption

apply simp

done

done

lemma lr-of-tran-no-overlaps: assumes distinct ifs shows Inr t = (lr-of-tran rt fw ifs) \implies no-overlaps

OF-match-fields-unsafe t

apply (unfold lr-of-tran-def Let-def pack-OF-entries-def)

apply (simp split: if-splits)

apply (thin-tac t = -)

apply (drule distinct-of-prio-hlp)

apply (rule no-overlaps-lroft-s3-hlp[rotated])

subgoal by (simp add: asms)

subgoal by (simp add: o-assoc)

done

lemma sorted-lr-of-tran-s3-hlp: \( \forall x \in \text{set } f. \ \text{fst} \ x \leq a \implies b \in \text{set (lr-of-tran-s3} s f) \implies \text{fst} \ b \leq a \)

by (auto simp add: lr-of-tran-s3-def)
lemma \texttt{lr-of-tran-s3-Cons}: \texttt{lr-of-tran-s3 ifs \ (a#ard) = (}
\[(p, b, case a of simple-action.Accept \Rightarrow [\text{Forward } c] | \text{simple-action.Drop} \Rightarrow [])],
(p.r,(c,a)) \leftarrow [a], b \leftarrow simple-match-to-of-match r ifs) \odot \texttt{lr-of-tran-s3 ifs ard by(clarsimp simp: lr-of-tran-s3-def)}

lemma \texttt{sorted-lr-of-tran-s3}: \texttt{sorted-descending (map fst f) \implies sorted-descending (map fst (lr-of-tran-s3 s f))}
apply(induction f)
subgoal by(simp add: lr-of-tran-s3-def)
apply(clarsimp simp: lr-of-tran-s3-Cons map-concat comp-def)
apply(unfold sorted-descending-append)
apply(simp add: sorted-descending-alt rev-map sorted-lr-of-tran-s3-hlp sorted-const)
done

lemma \texttt{sorted-lr-of-tran-hlp}: \texttt{(ofe-prio ◦ split3 OFEntry)} = \texttt{fst by(simp add: fun-eq-iff comp-def split3-def)}

lemma \texttt{lr-of-tran-sorted-descending}: \texttt{Inr r = lr-of-tran rt fw ifs =⇒ sorted-descending (map ofe-prio r)}
apply(unfold lr-of-tran-def Let-def)
apply(simp split: if-splits)
apply(thin-tac r = -)
apply(unfold sorted-lr-of-tran-hlp pack-OF-entries-def split3-def [abs-def] fun-app-def map-map comp-def prod.case-distrib)
apply(simp add: fst-def [symmetric])
apply(rule sorted-lr-of-tran-s3)
apply(drule sorted-annotated [OF less-or-eq-imp-le, OF disjI1])
apply(simp add: o-assoc)
done

lemma \texttt{lr-of-tran-s1-split}: \texttt{lr-of-tran-s1 (a # rt) = (route2match a, output-iface (routing-action a)) # lr-of-tran-s1 rt by(unfold lr-of-tran-s1-def list.map, rule)}

lemma \texttt{route2match-correct}: \texttt{valid-prefix (routing-match a) \implies prefix-match-semantics (routing-match a) (p-dst p) \iff simple-matches (route2match a) (p)}
by(simp add: route2match-def simple-matches.simps match-ifaceAny match-iface-refl ipset-from-cidr-0 prefix-match-semantics-ipset-from-netmask2)

lemma \texttt{s1-correct}: \texttt{valid-prefixes rt =⇒ has-default-route (rt::(i::len) prefix-routing) =⇒ \exists rm ra. generalized-sfw (lr-of-tran-s1 rt) p = Some (rm,ra) \land ra = output-iface (routing-table-semantics rt (p-dst p))}
apply(induction rt)
apply(simp; fail)
apply(drule valid-prefixes-split)
apply(clarsimp)
apply(erule disjE)
subgoal for a rt
apply(case-tac a)
apply(rename-tac routing-m metric routing-action)
apply(case-tac routing-m)
apply(simp add: valid-prefix-def pfvm-mask-def prefix-match-semantics-def generalized-sfw-def lr-of-tran-s1-def route2match-def simple-matches.simps match-ifaceAny match-iface-refl ipset-from-cidr-0 max-word-mask[where a = 'i, symmetric, simplified])
done

subgoal
apply(rule conjI)
apply(simp add: generalized-sfw-def lr-of-tran-s1-def route2match-correct; fail)
apply(simp add: route2match-def simple-matches.simps prefix-match-semantics-ipset-from-netmask2)
\begin{align*}
\text{definition to-OF-action } a & \equiv (\text{case } a \text{ of } (p,d) \Rightarrow (\text{case } d \text{ of } \text{simple-action.Accept} \Rightarrow [\text{Forward } p] \mid \text{simple-action.Drop} \Rightarrow [])) \\
\text{definition from-OF-action } a & = (\text{case } a \text{ of } [] \Rightarrow ("",\text{simple-action.Drop}) \mid [\text{Forward } p] \Rightarrow (p, \text{simple-action.Accept}))
\end{align*}

\text{lemma OF-match-linear-not-noD: } \text{OF-match-linear } \gamma \text{ p } \neq \text{NoAction} \implies \exists \text{ome. ome } \in \text{set oms } \land \gamma (\text{ofe-fields ome}) p
\begin{align*}
\text{apply(induction oms)} \\
\text{apply(simp)} \\
\text{apply(simp split: if-splits)} \\
\text{apply blast+}
\end{align*}

\text{done}

\text{lemma s3-noaction-hlp: } [\text{simple-match-valid ac; } \neg \text{simple-matches ac p; match-iface (oiface ac) (p-oiface p)}] \implies \text{OF-match-linear OF-match-fields-safe (map } (\lambda x. \text{split3 OFEntry } (x1, x, \text{case } ba \text{ of } \text{simple-action.Accept} \Rightarrow [\text{Forward } ad] \mid \text{simple-action.Drop} \Rightarrow [])) (\text{simple-match-to-of-match ac ifs)}) p = \text{NoAction}
\begin{align*}
\text{apply(rule ccontr)} \\
\text{apply(drule OF-match-linear-not-noD)} \\
\text{apply(clarsimp)} \\
\text{apply(rename-tac x)} \\
\text{apply(subgoal-tac all-prerequisites x)} \\
\text{apply(simp add: split3-def)} \\
\text{apply(subst(asm) of-match-fields-safe-eq2)} \\
\text{apply(simp:fail)+}
\end{align*}

\text{using simple-match-to-of-match-generates-prereqs by blast}

\text{lemma s3-correct:}
\begin{align*}
\text{assumes vsfwm: list-all simple-match-valid (map } (\text{fst } \circ \text{snd}) \text{ ard}) \\
\text{assumes ippkt: } p-\text{l2type p} = 0x800 \\
\text{assumes iifs: } p-\text{iface p } \in \text{ set ifs} \\
\text{assumes oiifs: list-all } (\lambda m. \text{oiface (fst (snd m))} = \text{ifaceAny}) \text{ ard} \\
\text{shows } \text{OF-match-linear OF-match-fields-safe (pack-OF-entries ifs ard) p } = \text{Action ao } \iff (\exists r \text{ af. generalized-sfw (map snd ard) p } = (\text{Some (r,af)} \land (\text{if snd af } = \text{simple-action.Drop} \text{ then ao } = [] \text{ else ao } = [\text{Forward (fst af)}])))
\end{align*}

\text{unfolding pack-OF-entries-def lr-of-tran-s3-def fan-app-def}
\text{using vsfwm oiifs}
\begin{align*}
\text{apply(induction ard)} \\
\text{subgoal by(simp add: generalized-sfw-simps)} \\
\text{apply simp} \\
\text{apply(clarsimp simp add: generalized-sfw-simps split: prod.splits)} \\
\text{apply(intro conjI)} \\
\text{subgoal for ard x1 ac ad ba} \\
\text{apply(clarsimp simp add: OF-match-linear-append split: prod.splits)} \\
\text{apply(drule simple-match-to-of-matchI[rotated])} \\
\text{apply(rule iifs)} \\
\text{apply(rule ippkt)} \\
\text{apply blast} \\
\text{apply(clarsimp simp add: comp-def)} \\
\text{apply(drule OF-match-linear-match-allsameaction[where } \\
\gamma=\text{OF-match-fields-safe and pri } = x1 \text{ and} \\
\text{oms } = \text{simple-match-to-of-match ac ifs and} \\
\text{act } = \text{case ba of simple-action.Accept } \Rightarrow [\text{Forward ad] } \ | \ \text{simple-action.Drop } \Rightarrow []])
\end{align*}
apply (unfold OF-match-fields-safe-def comp-def)
apply (erule Some-to-the[symmetric]; fail)
apply (clarsimp)
apply (intro iffI)

subgoal
apply (clarsimp simp: split3-def split: simple-action.splits flowtable-behavior.splits if-splits)
done

subgoal
apply (clarsimp simp: match-ifaceAny; fail)
done
done

subgoal for ard x1 ac ad ba
apply (simp add: OF-match-linear-append OF-match-fields-safe-def comp-def)
apply (clarify)
apply (rule subgoal-tac OF-match-linear OF-match-fields-safe (λx. split3 OFEntry (x1, x, case ba of simple-action.Accept ⇒ [Forward ad | simple-action.Drop ⇒ []]) (simple-match-to-of-match ac ifs)) p = NoAction)
apply (clarsimp)
apply (erule (1) s3-noaction-hlp)
apply (simp add: match-ifaceAny; fail)
done
done

done

done

done

done

done

done

done

context
notes valid-prefix-00 [simp, intro!]
begin

lemma lr-of-tran-s1-valid: valid-prefixes rt =⇒ gsfw-valid (lr-of-tran-s1 rt)
unfolding lr-of-tran-s1-def route2match-def gsfw-valid-def list-all-iff
apply (clarsimp simp: simple-match-valid-def valid-prefix-fw-def)
apply (intro conjI)
apply force
apply (simp add: valid-prefixes-alt-def)
done

end

lemma simple-match-valid-fbs-rlen: [valid-prefixes rt; simple-fw-valid fw; (a, aa, ab, b) ∈ set (annotate-rlen (lr-of-tran-fbs rt fw ifs))] =⇒ simple-match-valid aa
proof (goal_cases)
case 1
  note 1 [unfolded lr-of-tran-fbs-def Let-def]
  have gsfu-valid (map simple-rule-dtor fw) using gsfw-validI 1 by blast
  moreover have gsfu-valid (lr-of-tran-s1 rt) using 1 lr-of-tran-s1-valid by blast
  ultimately have gsfu-valid (generalized-fw-join (lr-of-tran-s1 rt) (map simple-rule-dtor fw)) using gsfw-join-valid by blast
  moreover have (aa, ab, b) ∈ set (lr-of-tran-fbs rt fw ifs) using 1 using in-annotate-rlen by fast
  ultimately show ?thesis unfolding lr-of-tran-fbs-def Let-def gsfw-valid-def list-all-iff by fastforce
qed

lemma simple-match-valid-fbs: [valid-prefixes rt; simple-fw-valid fw] =⇒ list-all simple-match-valid (map fst (lr-of-tran-fbs rt fw ifs))

32
proof \(\{\text{goal-cases}\}\)

case \(1\)

note \(1\) [unfolded \(\text{lr-of-tran-fbs-def}\) \(\text{Let-def}\)]

have \(\text{gsfu-valid} (\text{map simple-rule-dtor} \, \text{fw})\) using \(\text{gsfu-validI} \, 1\) by \(\text{blast}\)

moreover have \(\text{gsfu-valid} (\text{lr-of-tran-s1} \, \text{rt})\) using \(1 \, \text{lr-of-tran-s1-valid}\) by \(\text{blast}\)

ultimately have \(\text{gsfw-valid} (\text{generalized-fw-join} (\text{lr-of-tran-s1} \, \text{rt}) \, (\text{map simple-rule-dtor} \, \text{fw}))\) using \(\text{gsfw-join-valid}\) by \(\text{blast}\)

thus \(\text{thesis}\)

unfolding \(\text{lr-of-tran-fbs-def}\) \(\text{Let-def}\) \(\text{gsfw-valid-def}\) \(\text{list-all-iff}\) by \(\text{fastforce}\)

qed

lemma \(\text{lr-of-tran-prereqs}: \text{valid-prefixes} \, \text{rt} \implies \text{simple-fw-valid} \, \text{fw} \implies \text{lr-of-tran} \, \text{rt} \, \text{fw} \, \text{ifs} = \text{Inr} \, \text{oft} \implies \text{list-all} (\text{all-prerequisites} \circ \text{ofe-fields}) \, \text{oft}\)

unfolding \(\text{lr-of-tran-def}\) \(\text{pack-OF-entries-def}\) \(\text{lr-of-tran-s3-def}\) \(\text{Let-def}\)

apply \(\text{simp add: map-concat comp-def prod.case-distrib split3-def split: if-splits}\)

apply \(\text{clarsimp simp add: list-all-iff}\)

apply \(\text{drule simple-match-valid-fbs-rlen [rotated]}\)

apply \(\text{simp add: list-all-iff}; \text{fail}\)

apply \(\text{simp add: list-all-iff}; \text{fail}\)

apply \(\text{rule simple-match-to-of-match-generates-prereqs}; \text{assumption}\)

done

lemma \(\text{OF-unsafe-safe-match3-eq}:\)

\(\text{list-all} (\text{all-prerequisites} \circ \text{ofe-fields}) \, \text{oft}\)

unfolding \(\text{OF-priority-match-def}[\text{abs-def}]\)

proof \(\{\text{goal-cases}\}\)

case \(1\)

from \(1\) have \(\forall \, \text{packet}. \, [f \leftarrow \text{oft} \, . \, \text{OF-match-fields-unsafe} (\text{ofe-fields} \, f) \, \text{packet}] = [f \leftarrow \text{oft} \, . \, \text{OF-match-fields-safe} (\text{ofe-fields} \, f) \, \text{packet}]\)

apply \(\text{clarsimp simp add: list-all-iff \, OF-match-fields-safe-eq}\)

using \(\text{OF-match-fields-safe-eq}\) by \(\text{metis (mono-tags, lifting filter-cong)}\)

thus \(\text{case}\) by \(\text{metis}\)

qed

lemma \(\text{OF-unsafe-safe-match-linear-eq}:\)

\(\text{list-all} (\text{all-prerequisites} \circ \text{ofe-fields}) \, \text{oft}\)

unfolding \(\text{fun-eq-iff}\)

by \(\text{(induction oft)}\) \(\text{clarsimp simp add: list-all-iff \, OF-match-fields-safe-eq}\)+

lemma \(\text{simple-action-ne}\) \(\text{simp}\):

\(b \neq \text{simple-action.} \, \text{Accept} \iff \text{simple-action.} \, \text{Drop}\)

\(b \neq \text{simple-action.} \, \text{Drop} \iff \text{simple-action.} \, \text{Accept}\)

using \(\text{simple-action.} \, \text{exhaust by blast}\+)

lemma \(\text{map-snd-apfst}: \text{map snd} (\text{map} (\text{apfst} \, x) \, l) = \text{map snd} \, l\)

unfolding \(\text{map-map comp-def snd-apfst .}\)

lemma \(\text{match-iface\text{Any-eq}}: \text{ofiface} \, m = \text{iface\text{Any}} \implies \text{simple-matches} \, m \, p = \text{simple-matches} \, m \, (p \circ \text{p-ofiface := any})\)

by \(\text{(cases m)}\) \(\text{simp add: simple-matches.simps match-iface\text{Any}}\)

lemma \(\text{no-of-matchD}: \text{no-of-match} \, \text{fw} \implies \text{simple-fw} \, \text{fw} \, p = \text{simple-fw} \, \text{fw} \, (p \circ \text{p-ofiface := any})\)

by \(\text{(induction fw)}\)

(auto \text{simp add: no-of-match-def simple-fw-alt dest: match-iface\text{Any-eq}})
lemma lr-of-tran-fbs-acceptD:
  assumes s1: valid-prefixes rt has-default-route rt
  assumes s2: no-oif-match fw
  shows generalized-sfw (lr-of-tran-fbs rt fw ifs) p = Some (r, oif, simple-action.Accept) \implies
  simple-linux-router-nol12 rt fw p = Some (p[p-oiface := oif])
proof
  (goal-cases)
  case I
  note \[\{unfolded lr-of-tran-fbs-def Let-def nud ifupdateirrel split\}
  by simple-fw-iff-generalized-fw-accept split
  show \?case unfolding simple-linux-router-nol12-def by simp add: Let-def ifupdateirrel sfw oif ra rmra split: Option.bind-splits option.splits
  qed

lemma lr-of-tran-fbs-acceptI:
  assumes s1: valid-prefixes rt has-default-route rt
  assumes s2: no-oif-match fw
  shows simple-linux-router-nol12 rt fw p = Some (p[p-oiface := oif]) \implies
  \exists r. generalized-sfw (lr-of-tran-fbs rt fw ifs) p = Some (r, oif, simple-action.Accept)
proof
  (goal-cases)
  from s2 have nud: \(\forall p. \) simple-fw fw p \neq Undecided by (metis has-default-policy state.distinct(1))
  note ifupdateirrel = no-oif-matchD[OF s2(1), symmetric]
  case I
  from I have simple-fw fw p = Decision FinalAllow by simp add: simple-linux-router-nol12-def Let-def nud ifupdateirrel split: Option.bind-splits state.splits final-decision.splits
  then obtain r where r: generalized-sfw (map simple-rule-dtor fw) p = Some (r, simple-action.Accept) using simple-fw-if-generalized-fw-accept by blast
  have oif-def: oif = output-iface (routing-table-semantics rt (p-dst p))\ using I by(cases p) (simp add: simple-linux-router-nol12-def Let-def nud ifupdateirrel split: Option.bind-splits state.splits final-decision.splits)
  note s1-correct[OF s1, of p] then guess rm .. then guess ra .. note rmra = this
  show \?case unfolding lr-of-tran-fbs-let-def Let-def
  apply(rule exI)
  apply(rule generalized-fw-joinI)
  unfolding oif-def using rmra apply simp
  apply(rule r)
  done
  qed

lemma lr-of-tran-fbs-dropD:
  assumes s1: valid-prefixes rt has-default-route rt
  assumes s2: no-oif-match fw
  shows generalized-sfw (lr-of-tran-fbs rt fw ifs) p = Some (r, oif, simple-action.Drop) \implies
  simple-linux-router-nol12 rt fw p = None
proof (goal-cases)
  note ifupdateirrel = no-oif-matchD[OF s2(1), symmetric]
  case I
  from I[unfolded lr-of-tran-fbs-def Let-def, THEN generalized-fw-joinD]
  obtain \(\tau r f\) where generalized-sfw (lr-of-tran-s1 rt) p = Some (\(\tau r, oif\) \&
by prebusher

hence \( \exists u. \) simple-fw \( f_u \) \( p(\text{if} \text{-} \text{iface} \equiv u) = \) DecisionFinalDeny unfolding ifupdateirrel

using simple-fw-iff-generalized-fw-drop by blast

show \(?thesis \)

by(clarsimp simp: simple-linux-router-nol12-def Let-def split: Option.bind-splits)

qed

lemma \( \text{lr-of-tran-fbs-dropI} \):

assumes \( s1 \): valid-prefixes \( r \) has-default-route \( r \)

assumes \( s2 \): no-oif-match \( f_w \) has-default-policy \( f_w \)

shows simple-linux-router-nol12 \( r \) \( f_w \) \( p = \) None \( \implies \)

\( \exists r \) oif. generalized-sfw (\( \text{lr-of-tran-fbs} \) \( r \) \( f_w \) \( \text{ifs} \)) \( p = \) Some (\( r \), oif, simple-action.Drop)

proof(goal-cases)

from \( s2 \) have nud: \( \\exists \, p. \) simple-fw \( f_w \) \( p \neq \) Undecided by (metis has-default-policy state.distinct(1))

note ifupdateirrel = no-oif-matchD[OF s2(1), symmetric]

case 1

from 1 have simple-fw \( f_w \) \( p = \) DecisionFinalDeny by(simp add: simple-linux-router-nol12-def Let-def nud ifupdateirrel split: Option.bind-splits state.splits final-decision.splits)

then obtain \( r \) where \( r \): generalized-sfw (map simple-rule-dtor \( f_w \)) \( p = \) Some (\( r \), simple-action.Drop) using simple-fw-iff-generalized-fw-drop by blast

note s1-correct[OF s1, of p] then guess rm .. then guess ra .. note rmra = this

show \(?case unfolding \( \text{lr-of-tran-fbs-dropI} \) Let-def

apply(rule exI)

apply(rule exI[where \( x = ra \)])

apply(rule generalized-fw-join)

using rmra apply simp

apply(rule r)

done

qed

lemma \( \text{no-oif-match-fbs} \):

\( \text{no-oif-match \( f_w \)} \implies \) list-all \( (\lambda m. \text{iface} (\text{fst (snd \( m \))}) = \text{ifaceAny}) (\text{map (apfst of-nat}) (\text{annotate-rlen (\( \text{lr-of-tran-fbs} \) \( r \) \( f_w \) \( \text{ifs} \))})) \)

proof(goal-cases)

case 1

have c: \( \\exists mr \, ar \, mf \, af \, f \, a. \) \( [(mr, ar)] \in \) set (\( \text{lr-of-tran-s1} \) \( r \)); \( (mf, af) \in \) simple-rule-dtor \( \\text{set} \) \( f_w \); \( \text{simple-match-and} \) \( mr \) \( mf \)

= Some \( a \) \( \implies \) \( \text{iface} \) \( a \) = \text{ifaceAny}

proof(goal-cases)

case 1 \( mr \) of \( f \) anf \( f \) a

have \( \text{iface} \) \( mr \) = \text{ifaceAny} using 1(1) unfolding \( \text{lr-of-tran-s1-def route2match-def} \) by(clarsimp simp add: Set.image-iff)

moreover have \( \text{iface} \) \( mf \) = \text{ifaceAny} using 1(2) (no-oif-match \( f_w \)) unfolding no-oif-match-def simple-rule-dtor-def[abs-def]

by(clarsimp simp: list-all-iff split: simple-rule.splits) fastforce

ultimately show \(?case using 1(3) by(cases a; cases mr; cases mf) (simp add: iface-conjunct-iface.Any split: option.splits)

qed

have l: list-all \( (\lambda m. \text{iface} (\text{fst \( m \))) = \text{ifaceAny}) (\text{lr-of-tran-fbs} \) \( r \) \( f_w \) \( \text{ifs} \))

unfolding \( \text{lr-of-tran-fbs-def} \) Let-def list-all-iff

apply(clarify)

apply(subst(asm) generalized-sfw-join-set)

apply(clarsimp)

using c by blast

thus \(?case
proof (goal-cases)
  case 1
  have s*: (λm. offace (fst (snd m)) = ifaceAny) = (λm. offace (fst m) = ifaceAny) ○ snd unfolding comp-def ..
  show ?case unfolding * list-all-map[symmetric] map-snd-apfst map-snd-annotate-rlen using la .
  qed

qed

lemma lr-of-tran-correct:
  fixes p :: (32, 'a) simple-packet-ext-scheme
  assumes nerr: lr-of-tran rt fw ifs = Ifv
  and ipkt: p-l2type p = 0x800
  and ifd: p-iface p ∈ set ifs
  shows OF-priority-match OF-match-fields-safe oft p = Action [Forward oif] ←→ simple-linux-router-nol12 rt fw p = (Some
  (p[p-iface := oif])
  OF-priority-match OF-match-fields-safe oft p = Action ls → length ls ≤ 1
  ∃ls. length ls ≤ 1 ∧ OF-priority-match OF-match-fields-safe oft p = Action ls
  proof
    have s1: valid-prefixes rt has-default-route rt
    and s2: has-default-policy fw simple-fw-valid fw no-of-match fw
    and dfs: distinct ifs
    using nerr unfolding lr-of-tran-def by(simp-all split: if-splits)
    have no-of-match fw using nerr unfolding lr-of-tran-def by(simp split: if-splits)
    note s2 = s2 this
    have unsafe-safe-eq:
      apply(subst OF-unsafe-safe-match3-eq (rule lr-of-tran-prereqs s1 s2 nerr refl)+)
      apply(subst OF-unsafe-safe-match-linear-eq (rule lr-of-tran-prereqs s1 s2 nerr refl)+)
    done
    fun-iff-unsafe-safe-eq by metis
    let ?ard = map (apfst ofnat) (annotate-rlen (lr-of-tran-fbs rt fw ifs))
    have oft-def: oft = pack-OF-entries ifs ?ard unfolding lr-of-tran-def Let-def by(simp split: if-splits)
    have vld: list-all simple-match-valid (map (fst o snd) ?ard)
      unfolding fun-app-def map-map[symmetric] snd-apfst map-snd-apfst map-snd-annotate-rlen using
      simple-match-valid-fbs[OF s1(1) s2(2)] .
    have s*: list-all (λm. offace (fst (snd m)) = ifaceAny) ?ard unfolding no-of-match-fbs[OF s2(3)] .
    have not-unde: λp. simple-fw fw p ≠ Undecided by (metis has-default-policy s2(1) state.simps(3))
    have w1-1: λoif. OF-match-linear OF-match-fields-safe oft p = Action [Forward oif] ⇒ simple-linux-router-nol12 rt fw
    p = Some (p[p-iface := oif])
    ∧ oif = output-iface (routing-table-semantics rt (p-dst p))
    proof[intro conjl, goal-cases]
    case {1 ofif}
    note s3-correct[OF vld ipkt ifold(1) * , THEN iffD1, unfolded oft-def[symmetric], OF 1]
    hence ∃r. generalized-sfw (map snd (map (apfst ofnat) (annotate-rlen (lr-of-tran-fbs rt fw ifs)))) p = Some (r, (oif, simple-action.Accept))
    by(clarsimp split: if-splits)
    then obtain r where generalized-sfw (lr-of-tran-fbs rt fw ifs) p = Some (r, (oif, simple-action.Accept))
    unfolding map-map-comp-def snd-apfst map-snd-annotate-rlen by blast
thus \(\text{?case using lr-of-tran-fbs-acceptD}(\text{OF} s1 s2(3))\) by metis
thus \(\text{oif} = \text{output-iface} (\text{routing-table-semantics} \text{ rt} (\text{p-dst} \text{ p}))\)
  by(cases \text{p}) (clarsimp simp: simple-linux-router-nol12-def Let-def not-undec split: Option.bind-splits state.splits final-decision.splits)
qed
have \(\text{w1-2: } \bigwedge \text{oif}. \text{simple-linux-router-nol12} \text{ rt} \text{ fw} \text{ p} = \text{Some} (\text{p}((\text{p-oiface} := \text{oif}))) \implies \text{OF-match-linear} \text{ OF-match-fields-safe}\)
oft p = \text{Action} [\text{Forward oif}]
proof \(\text{goal-cases}\)
case \(1 \text{oif}\)
  note \(\text{lr-of-tran-fbs-acceptI}(\text{OF} s1 s2(3) \text{ s2}(1) \text{ this}, \text{ of ifs})\) then guess \(r \ldots\)
  note \(r = \text{this}\)
  hence \(\text{generalized-sfw} (\text{map snd (map (apfst-of-nat) \{annotate-rlen (lr-of-tran-fbs rt fw ifs)})}) \text{ p} = \text{Some} (r, (\text{oif}, \text{simple-action}.\text{Accept}))\)
    unfolding \text{map-snd-apfst map-snd-annotate-rlen}.
  moreover note \(s3\text{-correct}[\text{OF vld ippkt ifold}(1) \ast, \text{THEN iffD2, unfolded oft-def[\text{symmetric}], of}] [\text{Forward oif}]\)
  ultimately show \(\text{?case by simp}\)
qed
show \(\text{w1: } \bigwedge \text{oif}. (\text{OF-priority-match} \text{ OF-match-fields-safe} \text{ oft p} = \text{Action} [\text{Forward oif}]) = (\text{simple-linux-router-nol12 rt} \text{ fw p} = \text{Some} (\text{p}((\text{p-oiface} := \text{oif}))))\)
  unfolding \text{lin} using \(\text{w1-1} \text{ w1-2}\) by blast
show \(\text{w2: } (\text{OF-priority-match} \text{ OF-match-fields-safe} \text{ oft p} = \text{Action} []) = (\text{simple-linux-router-nol12 rt} \text{ fw p} = \text{None})\)
unfolding \text{lin}
proof \(\text{rule iffI, goal-cases}\)
case \(1\)
  note \(s3\text{-correct}[\text{OF vld ippkt ifold}(1) \ast, \text{THEN iffD1, unfolded oft-def[\text{symmetric}], OF}] [1]\)
  then obtain \(r \text{ oif where} \text{ roif} : \text{generalized-sfw} (\text{lr-of-tran-fbs rt fw ifs}) \text{ p} = \text{Some} (r, \text{oif}, \text{simple-action}.\text{Drop})\)
    unfolding \text{map-snd-apfst map-snd-annotate-rlen by(clarsimp simp: if-splits)}
  note \(\text{lr-of-tran-fbs-dropD}(\text{OF} s1 s2(3) \text{ this})\)
  thus \(\text{?case} .\)
next
  case \(2\)
  note \(\text{lr-of-tran-fbs-dropI}(\text{OF} s1 s2(3) \text{ s2}(1) \text{ this}, \text{ of ifs})\) then
  obtain \(r \text{ oif where} \text{ generalized-sfw} (\text{lr-of-tran-fbs rt fw ifs}) \text{ p} = \text{Some} (r, \text{oif, simple-action}.\text{Drop})\) by blast
    hence \(\text{generalized-sfw} (\text{map snd (map (apfst-of-nat) \{annotate-rlen (lr-of-tran-fbs rt fw ifs)})}) \text{ p} = \text{Some} (r, \text{oif, simple-action}.\text{Drop})\)
      unfolding \text{map-snd-apfst map-snd-annotate-rlen}.
    moreover note \(s3\text{-correct}[\text{OF vld ippkt ifold}(1) \ast, \text{THEN iffD2, unfolded oft-def[\text{symmetric}], of}] [\text{[]}\)
      ultimately show \(\text{?case by force}\)
qed
have \(\text{br-determ: } \bigwedge \text{a}. \text{simple-linux-router-nol12} \text{ rt} \text{ fw p} = \text{Some} \text{ a} \implies \text{ a} = \text{p}((\text{p-oiface} := \text{output-iface} (\text{routing-table-semantics} \text{ rt} (\text{p-dst} \text{ p}))))\)
  by(clarsimp simp: simple-linux-router-nol12-def Let-def not-undec split: Option.bind-splits state.splits final-decision.splits)
show notno: \(\text{OF-priority-match} \text{ OF-match-fields-safe} \text{ oft p} \neq \text{NoAction}\)
apply(cases simple-linux-router-nol12 rt fw p)
using w2 apply(simp)
using w1[\text{of output-iface} (\text{routing-table-semantics} \text{ rt} (\text{p-dst} \text{ p}))] apply(simp)
apply(drule br-determ)
apply(simp)
done
show notub: \(\text{OF-priority-match} \text{ OF-match-fields-safe} \text{ oft p} \neq \text{Undefined}\) unfolding \text{lin} using \(\text{OF-match-linear-ne-Undefined}\) .
show notmult: \(\bigwedge \text{ls}. \text{OF-priority-match} \text{ OF-match-fields-safe} \text{ oft p} = \text{Action} \text{ ls} \implies \text{length} \text{ ls} \leq 1\)
apply(cases simple-linux-router-nol12 rt fw p)
using w2 apply(simp)
using w1[\text{of output-iface} (\text{routing-table-semantics} \text{ rt} (\text{p-dst} \text{ p}))] apply(simp)
apply (drule lr-determ)
apply (clarsimp)
done

show \( \exists \text{ls}. \quad \text{length ls} \leq 1 \land \text{OF-priority-match OF-match-fields-safe oft p} = \text{Action ls} \)
apply (cases OF-priority-match OF-match-fields-safe oft p)
using notmult apply blast
using notno apply blast
using notub apply blast
done
qed

end

theory OF-conv-test
imports
  Iptables-Semantics.Parser
  Simple-Firewall.SimpleFw-toString
  Routing.IpRoute-Parser
  ../../LinuxRouter-OpenFlow-Translation
  ../../OpenFlow-Serialize
begin

parse-iptables-save SQRL-fw=iptables−save

term SQRL-fw
thm SQRL-fw-def
thm SQRL-fw-FORWARD-default-policy-def

value [code] map (\(\lambda (c, rs). (c, map (quote-rewrite o common-primitive-rule-toString) rs))\) SQRL-fw

definition unfolded = unfold-ruleset-FORWARD SQRL-fw-FORWARD-default-policy (map-of-string-ipv4 SQRL-fw)

lemma map (quote-rewrite o common-primitive-rule-toString) unfolded =
  ["'−p icmp −j ACCEPT'" ,
  "−i sl−lan −p tcp −m tcp −−spts [1024:65535] −m tcp −−dpts [80] −j ACCEPT'" ,
  "−i sl−wan −p tcp −m tcp −−spts [80] −m tcp −−dpts [1024:65535] −j ACCEPT'" ,
  "−j DROP"] by eval

lemma length unfolded = 4 by eval

value [code] map (quote-rewrite o common-primitive-rule-toString) (upper-closure unfolded)
lemma length (upper-closure unfolded) = 4 by eval

value [code] upper-closure (packet-assume-new unfolded)

lemma length (lower-closure unfolded) = 4 by eval

lemma check-simple-fw-preconditions (upper-closure unfolded) = True by eval
lemma \( \forall m \in \text{get-match'set} \quad (\text{upper-closure (packet-assume-new unfolded)}, \text{normalized-nnf-match m}) \) by eval
lemma \( \forall m \in \text{get-match'set} \quad (\text{optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new unfolded))}, \text{normalized-nnf-match m}) \) by eval

38
lemma check-simple-fw-preconditions (upper-closure (optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new unfolded)))) by eval

lemma length (to-simple-firewall (upper-closure (packet-assume-new unfolded))) = 4 by eval

lemma (lower-closure (optimize-matches abstract-for-simple-firewall (lower-closure (packet-assume-new unfolded)))) = lower-closure unfolded

lower-closure unfolded = upper-closure unfolded

(upper-closure (optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new unfolded)))) = upper-closure unfolded by eval+

value[code] (getParts (to-simple-firewall (lower-closure (optimize-matches abstract-for-simple-firewall (lower-closure (packet-assume-new unfolded))))))

definition SQRL-fw-simple ≡ rendups-rev (to-simple-firewall (upper-closure (optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new unfolded)))))

value[code] SQRL-fw-simple

lemma simple-fw-valid SQRL-fw-simple by eval

parse-ip-route SQRL-rtbl-main = ip-route

value SQRL-rtbl-main = \{(routing-match = PrefixMatch 0xA000100 24, metric = 0, routing-action = λ(output-iface = "s1–lan", next-hop = None))\}, \{(routing-match = PrefixMatch 0xA000200 24, metric = 0, routing-action = λ(output-iface = "s1–wan", next-hop = None))\}, \{(routing-match = PrefixMatch 0 0, metric = 0, routing-action = λ(output-iface = "s1–wan", next-hop = Some 0x1000201))\} by eval

value dotdecimal-of-ipvaddr 0xA0D2500

lemma SQRL-rtbl-main = |
rr-ctor (10,0,1,0) 24 "s1–lan" None 0,
rr-ctor (10,0,2,0) 24 "s1–wan" None 0,
rr-ctor (0,0,0,0) 0 "s1–wan" (Some (10,0,2,1)) 0
|
by eval

definition SQRL-rtbl-main-sorted ≡ rev (sort-key (λr. pfxm-length (routing-match r)) SQRL-rtbl-main)

value SQRL-rtbl-main-sorted

definition SQRL-ifs ≡ |
(iface-name = "s1–lan", iface-mac = 0x10001),
(iface-name = "s1–wan", iface-mac = 0x10002)
|

value SQRL-ifs

definition SQRL-macs ≡ |
("s1–lan", ip4addr-of-dotdecimal (10,0,1,2), 0x1),
("s1–lan", ip4addr-of-dotdecimal (10,0,1,3), 0x2),
("s1–wan", ip4addr-of-dotdecimal (10,0,2,1), 0x3)
|

value SQRL-macs

definition SQRL-ports ≡ |
("s1–lan", "1"),
("s1–wan", "1"),
lemma let fu = SQRL-fu-simple in no-oif-match fu \land has-default-policy fu \land simple-fu-valid fu by eval
lemma let rt = SQRL-rtbl-main-sorted in valid-prexes rt \land has-default-route rt by eval
lemma let ifs = (map iface-name SQRL-ifs) in distinct ifs by eval

definition of \equiv
\begin{align*}
& \text{case (br-of-tran SQRL-rtbl-main-sorted SQRL-fu-simple (map iface-name SQRL-ifs))} \\
& \text{of (Inr openflow-rules) } \Rightarrow \text{ map (serialize-of-entry (the \circ map-of SQRL-ports)) openflow-rules}
\end{align*}

lemma of =
\begin{align*}
& \text{"priority=x, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, action=output:2",} \\
& \text{"priority=11, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, action=output:2",} \\
& \text{"priority=10, hard-timeout=0, idle-timeout=0, in-port=1, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=1024 / 0x800, tp-dst=1024 / 0x800, action=drop",} \\
& \text{"priority=10, hard-timeout=0, idle-timeout=0, in-port=1, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=1024 / 0x800, tp-dst=1024 / 0x800, action=drop",} \\
& \text{"priority=10, hard-timeout=0, idle-timeout=0, in-port=1, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=8192 / 0x0000, tp-dst=8192 / 0x0000, action=drop",} \\
& \text{"priority=10, hard-timeout=0, idle-timeout=0, in-port=1, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=8192 / 0x0000, tp-dst=8192 / 0x0000, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
& \text{"priority=9, hard-timeout=0, idle-timeout=0, in-port=2, dl-type=0x800, nw-proto=1, nw-dst=10.0.2.0 / 24, tp-src=80, tp-dst=80, action=drop",} \\
\end{align*}

40
value [code] of

end
theory RFC2544
imports
Iptables-Semantics.Parser
Routing.IpRoute-Parser
../../LinuxRouter-OpenFlow-Translation
../../OpenFlow-Serialize

begin

parse-iptables-save SQRL-fw=iptables -save

term SQRL-fw
thm SQRL-fw-def
thm SQRL-fw-FORWARD-default-policy-def

value [code] map (λ (c, rs) (c, map (quote-rewrite o common-primitive-rule-toString) rs)) SQRL-fw

definition unfolded = unfold-ruleset-FORWARD SQRL-fw-FORWARD-default-policy (map-of-string-ipv4 SQRL-fw)

lemma length unfolded = 26 by eval

value [code] unfolded
value [code] (upper-closure unfolded)
value [code] map (quote-rewrite o common-primitive-rule-toString) (upper-closure unfolded)

lemma length (upper-closure unfolded) = 26 by eval

value [code] upper-closure (packet-assume-new unfolded)

lemma length (lower-closure unfolded) = 26 by eval

lemma check-simple-fw-preconditions (upper-closure unfolded) by eval
lemma ∀ m ∈ get-match’set (upper-closure (packet-assume-new unfolded)). normalized-nnf-match m by eval
lemma ∀ m ∈ get-match’set (optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new unfolded))). normalized-nnf-match m by eval

lemma check-simple-fw-preconditions (upper-closure (optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new unfolded)))) by eval

lemma length (to-simple-firewall (upper-closure (packet-assume-new unfolded))) = 26 by eval

lemma (lower-closure (optimize-matches abstract-for-simple-firewall (lower-closure (packet-assume-new unfolded)))) = lower-closure unfolded

lower-closure unfolded = upper-closure unfolded

(upper-closure (optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new unfolded)))) = upper-closure unfolded by eval+

value [code] (getParts (to-simple-firewall (lower-closure (optimize-matches abstract-for-simple-firewall (lower-closure (packet-assume-new unfolded)))))))
definition SQRL-fw-simple ≡ remdups-rev (to-simple-firewall (upper-closure (optimize-matches abstract-for-simple-firewall (upper-closure (packet-assume-new-unfolded)))))
value [code] SQRL-fw-simple
lemma simple-fw-valid SQRL-fw-simple by eval

parse-ip-route SQRL-rtbl-main = ip--route
value SQRL-rtbl-main
lemma SQRL-rtbl-main = [ routing-match = PrefizMatch 0xC6120100 24, metric = 0, routing-action = [output-iface = "ip1", next-hop = None] ],
[routing-match = PrefizMatch 0xC6130100 24, metric = 0, routing-action = [output-iface = "op1", next-hop = None] ],
[routing-match = PrefizMatch 0 0, metric = 0, routing-action = [output-iface = "op1", next-hop = Some 0xC6130102] ]
by eval
lemma SQRL-rtbl-main = [ rr-ctor (198, 18, 1, 0) 24 "ip1" None 0,
rr-ctor (198, 19, 1, 0) 24 "op1" None 0,
rr-ctor (0, 0, 0, 0) 0 "op1" (Some (198, 19, 1, 2)) 0 ]
by eval

definition SQRL-ports ≡ [ ["ip1", "1"],
["op1", "2"] ]

definition of ≡ case (br-of-tran SQRL-rtbl-main SQRL-fw-simple (map fst SQRL-ports)) of [map (serialize-of-entry (the o map-of SQRL-ports)) openflow-rules]
lemma of =
[ ["priority=27, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-dst=198.18.1.0/24, action=drop" ],
["priority=26, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-dst=198.19.1.0/24, action=drop" ],
["priority=25, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.1.1/32, nw-dst=192.18.101.1/32, action=drop" ],
["priority=24, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.2.2/32, nw-dst=192.18.102.2/32, action=drop" ],
["priority=23, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.3.3/32, nw-dst=192.18.103.3/32, action=drop" ],
["priority=22, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.4.4/32, nw-dst=192.18.104.4/32, action=drop" ],
["priority=21, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.5.5/32, nw-dst=192.18.105.5/32, action=drop" ],
["priority=20, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.6.6/32, nw-dst=192.18.106.6/32, action=drop" ],
["priority=19, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.7.7/32, nw-dst=192.18.107.7/32, action=drop" ],
["priority=18, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.8.8/32, nw-dst=192.18.108.8/32, action=drop" ],
["priority=17, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.9.9/32, nw-dst=192.18.109.9/32, action=drop" ],
["priority=16, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.10.10/32, nw-dst=192.18.110.10/32, action=drop" ],
["priority=15, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.11.11/32, nw-dst=192.18.111.11/32, action=drop" ],
["priority=14, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.12.12/32, nw-dst=192.18.112.12/32, action=drop" ],
["priority=13, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.19.1.1/32, nw-dst=192.19.65.1/32, action=drop" ],
["priority=12, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.13.13/32, nw-dst=192.18.113.13/32, action=drop" ],
["priority=11, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.14.14/32, nw-dst=192.18.114.14/32, action=drop" ],
["priority=10, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.15.15/32, nw-dst=192.18.115.15/32, action=drop" ],
["priority=9, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.16.16/32, nw-dst=192.18.116.16/32, action=drop" ],
["priority=8, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.17.17/32, nw-dst=192.18.117.17/32, action=drop" ],
["priority=7, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.18.18/32, nw-dst=192.18.118.18/32, action=drop" ],
["priority=6, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.19.19/32, nw-dst=192.18.119.19/32, action=drop" ],
["priority=5, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.20.20/32, nw-dst=192.18.120.20/32, action=drop" ],
["priority=4, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.21.21/32, nw-dst=192.18.121.21/32, action=drop" ],
["priority=3, hard-timeout=0, idle-timeout=0, dl-type=0x800, nw-src=192.18.22.22/32, nw-dst=192.18.122.22/32, action=drop" ],
value[code] length of

end
Part II
Documentation

1 Configuration Translation

All the results we present in this section are formalized and verified in Isabelle/HOL [11]. This means that their formal correctness can be trusted a level close to absolute certainty. The definitions and lemmas stated here are merely a repetition of lemmas stated in other theory files. This means that they have been directly set to this document from Isabelle and no typos or hidden assumptions are possible. Additionally, it allows us to omit various helper lemmas that do not help the understanding. However, it causes some notation inaccuracy, as type and function definitions are stated as lemmas or schematic goals.

theory OpenFlow-Documentation

1.1 Linux Firewall Model

We want to write a program that translates the configuration of a Linux firewall to that of an OpenFlow switch. We furthermore want to verify that translation. For this purpose, we need a clear definition of the behavior of the two device types – we need their models and semantics. In case of a Linux firewall, this is problematic because a Linux firewall is a highly complex device that is ultimately capable of general purpose computation. Creating a comprehensive semantics that encompasses all possible configuration types of a Linux firewall is thus highly non-trivial and not useful for the purpose of analysis. We decided to approach the problem from the other side: we created a model that includes only the most basic features. (This implies neglecting IPv6.) Fortunately, many of the highly complex features are rarely essential and even our basic model is still of some use.

We first divided the firewall into subsystems. Given a routing table \( rt \), the firewall rules \( fw \), the routing decision for a packet \( p \) can be obtained by \( \text{routing-table-semantics} \) \( rt \) \( (p-dst \ p) \), the firewall decision by \( \text{simple-fw} \) \( fw \) \( p \). We draft the first description of our Linux router model:

1. The destination MAC address of an arriving packet is checked: Does it match the MAC address of the ingress port? If it does, we continue, otherwise, the packet is discarded.

2. The routing decision \( rd \equiv \text{routing-table-semantics} \) \( rt \) \( p \) is obtained.

3. The packet’s output interface is updated based on \( rd^1 \).

4. The firewall is queried for a decision: \( \text{simple-fw} \) \( fw \) \( p \). If the decision is to Drop, the packet is discarded.

5. The next hop is computed: If \( rd \) provides a next hop, that is used. Otherwise, the destination address of the packet is used.

6. The MAC address of the next hop is looked up; the packet is updated with it and sent.

We decided that this description is best formalized as an abortable program in the option monad:

\[
\text{lemma simple-linux-router}\ rt\ \ fw\ \ mlf\ ifl\ p\ \equiv\ \{\ \\
\quad \text{-} \leftarrow \text{iface-packet-check}\ ifl\ p; \\
\quad \text{let}\ \ rd\ \equiv\ \text{routing-table-semantics}\ \ rt\ \ (p-dst\ p); \\
\quad \text{let}\ \ p = p[p-oiface := \text{output-iface}\ rd]; \\
\quad \text{let}\ \ fd\ \equiv\ \text{simple-fw}\ \ fw\ \ p; \\
\quad \text{-} \leftarrow \begin{cases} \\
\text{Decision FinalAllow} & \Rightarrow \text{Some} () \\
\text{Decision FinalDeny} & \Rightarrow \text{None} \\
\end{cases}; \\
\quad \text{let}\ \ nh = \begin{cases} \\
\text{case next-hop}\ \ rd\ \Rightarrow \text{Some} \ (p-dst\ p) | \text{Decision} \ \text{FinalDeny} \Rightarrow \text{None}; \\
\text{let}\ \ ma = \begin{cases} \\
\text{mlf}\ \ nh; \\
\text{Some}\ \ (p[p-l2dst := ma]) \\
\end{cases}
\}
\}
\]

\[
\text{unfolding}\ \ \text{fromMaybe-def}\ [\text{symmetric}]\ \ \text{by}\ (\text{fact simple-linux-router-def})
\]

where \( mlf \) is a function that looks up the MAC address for an IP address.

There are already a few important aspects that have not been modelled, but they are not core essential for the functionality of a firewall. Namely, there is no local traffic from/to the firewall. This is problematic since this model can not generate ARP replies — thus, an equivalent OpenFlow device will not do so, either. Furthermore, this model is problematic because it requires access to a function that looks up a MAC address, something that may not be known at the time of time running a translation to an OpenFlow configuration.

\[^1\text{Note that we assume a packet model with input and output interfaces. The origin of this is explained in Section 1.1.2}\]
It is possible to circumvent these problems by inserting static ARP table entries in the directly connected devices and looking up their MAC addresses a priori. A test-wise implementation of the translation based on this model showed acceptable results. However, we deemed the a priori lookup of the MAC addresses to be rather inelegant and built a second model.

**definition** simple-linux-router-altered rt fw ifl p ≡ do
let rd = routing-table-semantics rt (p-dst p);
let p = p(p-iface := output-interface rd);
- ← if p-iface p = p-iface p then None else Some ();
let fd = simple-fw fw p;
- ← (case fd of Decision FinalAllow ⇒ Some () | Decision FinalDeny ⇒ None);
Some p

In this model, all access to the MAC layer has been eliminated. This is done by the approximation that the firewall will be asked to route a packet (i.e. be addressed on the MAC layer) iff the destination IP address of the packet causes it to be routed out on a different interface. Because this model does not insert destination MAC addresses, the destination MAC address has to be already correct when the packet is sent. This can only be achieved by changing the subnet of all connected devices, moving them into one common subnet\(^2\).

While a test-wise implementation based on this model also showed acceptable results, the model is still problematic. The check p-iface p = p-iface p and the firewall require access to the output interface. The details of why this cannot be provided are be elaborated in Section 1.3. The intuitive explanation is that an OpenFlow match language to select a routing table. Based on our directive, we only focused on the single most used main routing table.

We define a routing table entry to be a record (named tuple) of a prefix match, a metric and the routing action, which in turn is a record of an output interface and an optional next-hop address.

**schematic-goal** (**?rtbl-entry**) : ('a::len) routing-rule = () routing-match = PrefixMatch pfx len, metric = met, routing-action = () output-interface = oif-string, next-hop = (h : ('a word option)) | |

A routing table is then a list of these entries:

**lemma** (rtbl : ('a :: len) prefix-routing) = (rtbl : 'a routing-rule list) by rule

Not all members of the type prefix-routing are sane routing tables. There are three different validity criteria that we require so that our definitions are adequate.

- The prefixes have to be 0 in bits exceeding their length.
- There has to be a default rule, i.e. one with prefix length 0. With the condition above, that implies that all its prefix bits are zero and it thus matches any address.
- The entries have to be sorted by prefix length and metric.

\(^2\)There are cases where this is not possible — A limitation of our system.
The first two are set into code in the following way:

\[
\text{lemma valid-prefix (PrefixMatch } pfx \text{ len) } \equiv \ pfx \ \&\& \ (2^{32 - \text{len}} - 1) = (0 :: 32 \ \text{word})
\]

\text{unfolding valid-prefix-def } \text{ pfzm-mask-def } \text{ mask-def by (simp add: word-bw-comms(1))}

\text{lemma has-default-route } rt \leftarrow (\exists r \in \text{set } rt. \text{ pfzm-length (routing-match } r) = 0)
\text{ by (fact has-default-route-alt)}

The third is not needed in any of the further proofs, so we omit it.

The semantics of a routing table is to simply traverse the list until a matching entry is found.

\text{schematic-goal routing-table-semantics (rt-entry} \# rt \text{)} dst-addr = (if prefix-match-semantics (routing-match rt-entry) dst-addr then routing-action rt-entry else routing-table-semantics rt dst-addr) \text{ by (fact routing-table-semantics.simps)}

If no matching entry is found, the behavior is undefined.

\subsection*{1.1.2 iptables Firewall}

The firewall subsystem in a linux router is not any less complex than any of the of the other systems. Fortunately, this complexity has been dealt with in [6, 5] already and we can directly use the result.

In short, one of the results is that a complex iptables configuration can be simplified to be represented by a single list of matches that only support the following match conditions:

- (String) prefix matches on the input and output interfaces.
- A prefix-match on the source and destination IP address.
- An exact match on the layer 4 protocol.
- Interval matches on the source or destination port, e.g. \( p_d \in \{1..0x3FF\} \)

The model/type of the packet is adjusted to fit that: it is a record of the fields matched on. This also means that input and output interface are coded to the packet. Given that this information is usually stored alongside the packet content, this can be deemed a reasonable model. In case the output interface is not needed (e.g., when evaluating an OpenFlow table), it can simply be left blank.

Obviously, a simplification into the above match type cannot always produce an equivalent firewall, and the set of accepted packets has to be over- or underapproximated. The reader interested in the details of this is strongly referred to [6]; we are simply going to continue with the result: \text{simple-fw}.

One property of the simplification is worth noting here: The simplified firewall does not know state and the simplification approximates stateful matches by stateless ones. Thus, the overapproximation of a stateful firewall ruleset that begins with accepting packets of established connections usually begins with a rule that accepts all packets. Dealing with this by writing a meaningful simplification of stateful firewalls is future work.

\subsection*{1.2 OpenFlow Switch Model}

In this section, we present our model of an OpenFlow switch. The requirements for this model are derived from the fact that it models devices that are the target of a configuration translation. This has two implications:

- All configurations that are representable in our model should produce the correct behavior wrt. their semantics. The problem is that correct here means that the behavior is the same that any real device would produce. Since we cannot possibly account for all device types, we instead focus on those that conform to the OpenFlow specifications. To account for the multiple different versions of the specification (e.g. [2, 3]), we tried making our model a subset of both the oldest stable version 1.0 [2] and the newest available specification version 1.5.1 [3].
- Conversely, our model does not need to represent all possible behavior of an OpenFlow switch, just the behavior that can be invoked by the result of our translation. This is especially useful regarding for controller interaction, but also for MPLS or VLANs, which we did not model in Section 1.1.

More concretely, we set the following rough outline for our model.

- A switch consists of a single flow table.
- A flow table entry consists of a priority, a match condition and an action list.
• The only possible action (we require) is to forward the packet on a port.

• We do not model controller interaction.

Additionally, we decided that we wanted to be able to ensure the validity of the flow table in all qualities, i.e. we want to model the conditions ‘no overlapping flow entries appear’, ‘all match conditions have their necessary preconditions’. The details of this are explained in the following sections.

1.2.1 Matching Flow Table entries

Table 3 of Section 3.1 of [2] gives a list of required packet fields that can be used to match packets. This directly translates into the type for a match expression on a single field:

\[
\text{schematic-goal} \quad (\text{field-match} :: \text{of-match-field}) \in \{ \\
\quad \text{IngressPort} (?i::\text{string}), \\
\quad \text{EtherSrc} (?a::48 \text{ word}), \text{EtherDst} (?ad::48 \text{ word}), \\
\quad \text{VlanId} (?i::16 \text{ word}), \text{VlanPriority} (?p::16 \text{ word}), \\
\quad \text{IPV4Src} (?pms::32 \text{ prefix-match}), \text{IPV4Dst} (?pmd::32 \text{ prefix-match}), \\
\quad \text{IPV4Proto} (?ipp :: 8 \text{ word}), \\
\quad \text{IPv4Src} (?ms :: 16 \text{ word}), \text{IPv4Dst} (?md :: 16 \text{ word}) \} \\
\text{by}(\text{fact of-match-field-typeset})
\]

Two things are worth additional mention: L3 and L4 “addresses”. The IPV4Src and IPV4Dst matches are specified as “can be subnet masked” in [2], whereas [3] states clearly that arbitrary bitmasks can be used. We took the conservative approach here. Our alteration of L4Src and L4Dst is more grave. While [2] does not state anything about layer 4 ports and masks, [3] specifically forbids using masks on them. Nevertheless, OpenVSwitch [1] and some other implementations support them. We will explain in detail why we must include bitmasks on layer 4 ports to obtain a meaningful translation in Section 1.3.

One of-match-field is not enough to classify a packet. To match packets, we thus use entire sets of match fields. As Guha et al. [7] noted, executing a set of given of-match-fields on a packet requires careful consideration. For example, it is not meaningful to use IPV4Dst if the given packet is not actually an IP packet, i.e. IPV4Dst has the prerequisite of EtherType 0x800 being among the match fields. Guha et al. decided to use the fact that the preconditions can be arranged on a directed acyclic graph (or rather: an acyclic forest).

They evaluated match conditions in a manner following that graph: first, all field matches without preconditions are evaluated. Upon evaluating a field match (e.g., EtherType 0x800), the matches that had their precondition fulfilled by it (e.g., IPV4Src and IPV4Src in this example) are evaluated. This mirrors the faulty behavior of some implementations (see [7]). Adopting that behavior into our model would mean that any packet matches against the field match set \{IPV4Dst (PrefixMatch 0x80808080 32)\} instead of just those destined for 8.8.8.8 or causing an error. We found this to be unsatisfactory.

To solve this problem, we made three definitions. The first, match-no-prereq matches an of-match-field against a packet without considering prequisites. The second, prerequisites, checks for a given of-match-field whether its prerequisites are in a set of given match fields. Especially:

\[ \text{prerequisites} (\text{VlanPriority pri}) \quad m = (\exists \text{ id. let } v = \text{VlanId id in } v \in m \land \text{prerequisites } v m) \]
\[ \text{prerequisites} (\text{IPV4Proto proto}) \quad m = (\text{let } v = \text{EtherType 0x8000 in } v \in m \land \text{prerequisites } v m) \]
\[ \text{prerequisites} (\text{IPV4Src a}) \quad m = (\text{let } v = \text{EtherType 0x8000 in } v \in m \land \text{prerequisites } v m) \]
\[ \text{prerequisites} (\text{IPV4Dst a}) \quad m = (\text{let } v = \text{EtherType 0x8000 in } v \in m \land \text{prerequisites } v m) \]

by(fact prerequisites.simps)+

Then, to actually match a set of of-match-field against a packet, we use the option type:

\[ \text{OF-match-fields} \quad m p = \]
\[ (\text{if } \exists f \in m. \neg \text{prerequisites } f m \text{ then None else } \text{if } \forall f \in m. \text{match-no-prereq } f p \text{ then Some True else Some False} ) \]

by(fact OF-match-fields-alt)

1.2.2 Evaluating a Flow Table

In the previous section, we explained how we match the set of match fields belonging to a single flow entry against a packet. This section explains how the correct
flow entry from a table can be selected. To prevent to much entanglement with the previous section, we assume an arbitrary match function $\gamma$. This function $\gamma$ takes the match condition $m$ from a flow entry *OFEntry priority m action* and decides whether a packet matches those.

The flow table is simply a list of flow table entries *flow-entry-match*. Deciding the right flow entry to use for a given packet is explained in the OpenFlow specification [2], Section 3.4:

Packets are matched against flow entries based on prioritization. An entry that specifies an exact match (i.e., has no wildcards) is always the highest priority. All wildcard entries have a priority associated with them. Higher priority entries must match before lower priority ones. If multiple entries have the same priority, the switch is free to choose any ordering.

We use the term “overlapping” for the flow entries that can cause a packet to match multiple flow entries with the same priority. Guha et al. [7] have dealt with overlapping. However, the semantics for a flow table they presented [7, Figure 5] is slightly different from what they actually used in their theory files. We have tried to reproduce the original inductive definition (while keeping our abstraction $\gamma$), in Isabelle/HOL:

**Lemma** $\gamma$ (ofe-fields $fe$) $p = True \implies \forall fe' \in \text{set } (ft1 @ ft2), \text{ ofe-prio } fe' > \text{ ofe-prio } fe \implies \gamma (\text{ofe-fields } fe') p = False \implies \text{guha-table-semantics } \gamma (ft1 @ fe \# ft2) p \ (\text{Some (ofe-action } fe))$

$\forall fe \in \text{set } ft, \gamma (\text{ofe-fields } fe) p = False \implies \text{guha-table-semantics } \gamma ft p \ \text{None by (fact guha-matched guha-unmatched)}$+

Guha et al. have deliberately made their semantics non-deterministic, to match the fact that the switch “may choose any ordering”. This can lead to undesired results:

**Lemma** $\text{CARD}('\text{action}') \geq 2 \implies \exists ff. \gamma ff p \implies \exists ft (a1 :: 'action), (a2 :: 'action), a1 \neq a2 \land \text{guha-table-semantics } \gamma ft p \ (\text{Some } a1) \land \text{guha-table-semantics } \gamma ft p \ (\text{Some } a2) \text{ by (fact guha-table-semantics-2x2res)}$

This means that, given at least two distinct actions exist and our matcher $\gamma$ is not false for all possible match conditions, we can say that a flow table and two actions exist such that both actions are executed. This can be misleading, as the switch might choose an ordering on some flow table and never execute some of the (overlapped) actions.

Instead, we decided to follow Section 5.3 of the specification [3], which states:

If there are multiple matching flow entries, the selected flow entry is explicitly undefined.

This still leaves some room for interpretation, but it clearly states that overlapping flow entries are undefined behavior, and undefined behavior should not be invoked. Thus, we came up with a semantics that clearly indicates when undefined behavior has been invoked:

**Lemma**

```
OF-priority-match $\gamma$ flow-entries packet = (
let $m = \text{filter } (\lambda f. \gamma (\text{ofe-fields } f) \text{ packet}) \text{ flow-entries};
$m' = \text{filter } (\lambda f. \forall fo \in \text{ set } m. \text{ ofe-prio } fo \leq \text{ ofe-prio } f) m\in
\text{ case } m' \text{ of }[] \Rightarrow \text{NoAction}
| [s] \Rightarrow \text{Action } (\text{ofe-action } s)
| - \Rightarrow \text{Undefined})
```

**Unfolding** **OF-priority-match-def** ..

The definition works the following way:

1. The flow table is filtered for those entries that match, the result is called $m$.
2. $m$ is filtered again, leaving only those entries for which no entries with lower priority could be found, i.e. the matching flow table entries with minimal priority. The result is called $m'$.
3. A case distinction on $m'$ is made. If only one matching entry was found, its action is returned for execution. If $m$ is empty, the flow table semantics returns *NoAction* to indicate that the flow table does not decide an action for the packet. If, not zero or one entry is found, but more, the special value *Undefined* for indicating undefined behavior is returned.

---

$^4$This behavior has been deprecated.

$^5$The original is written in Coq [4] and we can not use it directly.

$^6$Note that the order of the flow table entries is irrelevant. We could have made this definition on sets but chose not to for consistency.
The use of *Undefined* immediately raises the question in which condition it cannot occur. We give the following definition:

**lemma** check-no-overlap \( \gamma \) \( ft \) = (\( \forall a \in \text{set } ft. \forall b \in \text{set } ft. (a \neq b \land \text{ofe-prio } a = \text{ofe-prio } b) \rightarrow \neg (\exists p. \gamma (\text{ofe-fields } a) p \land \gamma (\text{ofe-fields } b) p) \)) unfolding check-no-overlap-alt

Together with distinctness of the flow table, this provides the absence of *Undefined*\(^7\):

**lemma** \( [\gamma \text{check-no-overlap } ft; \text{distinct } ft] \) \( \Rightarrow \) \( \text{OF-priority-match } \gamma \) \( ft \) \( p \neq \text{Undefined} \) by \( \text{simp add: no-overlapsI no-overlaps-not-undefined} \)

Given the absence of overlapping or duplicate flow entries, we can show two interesting equivalences. The first is the equality to the semantics defined by Guha et al.:

**lemma** \( [\gamma \text{check-no-overlap } ft; \text{distinct } ft] \) \( \Rightarrow \) \( \text{OF-priority-match } \gamma \) \( ft \) \( p = \text{option-to-ftb } d \leftrightarrow \text{guha-table-semantics } \gamma \) \( ft \) \( p \) \( d \) by \( \text{simp add: guha-equal no-overlapsI} \)

where \( \text{option-to-ftb} \) maps between the return type of \( \text{OF-priority-match} \) and an option type as one would expect.

The second equality for \( \text{OF-priority-match} \) is one that helps reasoning about flow tables. We define a simple recursive traversal for flow tables:

**lemma**

\[ \begin{align*}
\text{OF-match-linear } \gamma \ [] p &= \text{NoAction} \\
\text{OF-match-linear } \gamma \ (a##as) p &= (\text{if } \gamma (\text{ofe-fields } a) p \text{ then Action (ofe-action } a) \text{ else OF-match-linear } \gamma \ as \ p) \\
&\text{by (fact OF-match-linear.simps)}+
\end{align*} \]

For this definition to be equivalent, we need the flow table to be sorted:

**lemma**

\[ [\text{no-overlaps } \gamma f; \text{sorted-descending } (\text{map ofe-prio } f)] \Rightarrow \text{OF-match-linear } \gamma \ f \ p = \text{OF-priority-match } \gamma \ f \ p \]

by (fact OF-eq)

As the last step, we implemented a serialization function for flow entries; it has to remain unverified. The serialization function deals with one little inaccuracy: We have modelled the *IngressPort* match to use the interface name, but OpenFlow requires numerical interface IDs instead. We deemed that pulling this translation step into the main translation would only make the correctness lemma of the translation more complicated while not increasing the confidence in the correctness significantly. We thus made replacing interface names by their ID part of the serialization.

Having collected all important definitions and models, we can move on to the conversion.

### 1.3 Translation Implementation

This section explains how the functions that are executed sequentially in a Linux firewall can be compressed into a single OpenFlow table. Creating this flow table in a single step would be immensely complicated. We thus divided the task into several steps using the following key insights:

- All steps that are executed in the Linux router can be formulated as a firewall, more specifically, a generalization of *simple-fw* that allows arbitrary actions instead of just accept and drop.
- A function that computes the conjunction of two *simple-fw* matches is already present. Extending this to a function that computes the join of two firewalls is relatively simple. This is explained in Section 1.3.1

#### 1.3.1 Chaining Firewalls

This section explains how to compute the join of two firewalls.

The basis of this is a generalization of *simple-fw*. Instead of only allowing *Accept* or *Drop* as actions, it allows arbitrary actions. The type of the function that evaluates this generalized simple firewall is *generalized-sfw*. The definition is straightforward:

**lemma**

\[ \text{generalized-sfw } [] p = \text{None} \]

\[ \text{generalized-sfw } (a \# as) p = (\text{if } (\text{case } a \text{ of } (m, -) \Rightarrow \text{simple-matches } m \ p) \text{ then Some } a \text{ else generalized-sfw as } p) \quad \text{by (fact generalized-sfw.simps)}+ \]

Based on that, we asked: if \( fw_1 \) makes the decision \( a \) (where \( a \) is the second element of the result tuple from *generalized-sfw*) and \( fw_2 \) makes the decision \( b \), how can we compute the firewall that makes the decision \( (a, b)\)\(^8\)?

One possible answer is given by the following definition:

\(^7\)It is slightly stronger than necessary, overlapping rules might be shadowed and thus never influence the behavior.

\(^8\)Note that tuples are right-associative in Isabelle/HOL, i.e., \((a, b, c)\) is a pair of \(a\) and the pair \((b, c)\)
Theorem \( \text{simple-fw-join} \text{I} \text{II} \equiv [(u, a, b) \iff (m_1, a) \iff \text{II}; (m_2, b) \iff \text{II}, u \iff \text{case simple-match-and m_1 m_2 of None} \Rightarrow \| | \text{Some s} \iff \| s]) \)

by (fact \( \text{generalized-fw-join-def} \text{[unfolded option2list-def]} + \text{abs-def} )

This definition validates the following lemma:

Lemma \( \text{generalized-fw-join} \text{I} \text{II} p = \text{Some} (u, d_1, d_2) \iff (\exists r_1, r_2, \text{generalized-fw-join} p = \text{Some} (r_1, d_1) \land \text{generalized-fw-join} p = \text{Some} (r_2, d_2) \land \text{Some} u = \text{simple-match-and r_1 r_2} ) \)

by (force dest: \text{generalized-fw-joinD} \text{generalized-fw-joinI} \text{[intro: Some-to-the symmetric]}

Thus, \( \text{generalized-fw-join} \) has a number of applications. For example, it could be used to compute a firewall ruleset that represents two firewalls that are executed in sequence.

Definition \( \text{simple-action-conj} a \ b \equiv (\text{if} \ a = \text{simple-action} \text{Accept} \land \ b = \text{simple-action} \text{Accept then simple-action} \text{Accept else simple-action} )\text{Drop} )\)

Definition \( \text{simple-rule-conj} \equiv (\text{uncurry SimpleRule} \circ \text{apsnd (uncurry simple-action-conj)}) \text{Drop} )\)

Theorem \( \text{simple-fw} r_{\text{S}} p = \text{Decision FinalAllow} \land \text{simple-fw} r_{\text{D}} p = \text{Decision FinalAllow} \iff (\text{map simple-rule-conj (generalized-fw-join map simple-rule-dtor r_{\text{S}})} (\text{map simple-rule-dtor r_{\text{D}}})) \text{p = Decision FinalAllow} \)

Unfolding \( \text{simple-rule-conj-def[abs-def]} \text{using simple-fw-join by (force simp add: comp-def apsnd-def map-prod-def case-prod-unfold uncurry-def[abs-def]}) \)

Using the join, it should be possible to compute any \( n \)-ary logical operation on firewalls. We will use it for something somewhat different in the next section.

1.3.2 Translation Implementation

This section shows the actual definition of the translation function, in Figure 1. Before beginning the translation, the definition checks whether the necessary preconditions are valid. This first two steps are to convert \( \text{fw} \) and \( \text{rt} \) to lists that can be evaluated by \( \text{generalized-sfw} \). For \( \text{fw} \), this is done by \( \text{map simple-rule-dtor} \), which just deconstructs \( \text{simple-rules} \) into tuples of match and action. For \( \text{rt} \), we made a firewall ruleset with rules that use prefix matches on the destination IP address. The next step is to join the two rulesets. The result of the join is a ruleset with rules \( r \) that only match if both, the corresponding firewall rule \( \text{fur} \) and the corresponding routing rule \( \text{rr} \) matches. The data accompanying \( r \) is the port from \( \text{rr} \) and the firewall decision from \( \text{fur} \). Next, descending priorities are added to the rules using \( \text{map (apfst word-of-nat) o annotate-rlen} \). If the number of rules is too large to fit into the \( 2^{16} \) priority classes, an error is returned. Otherwise, the function \( \text{pack-OF-entries} \) is used to convert the \( (16 \text{ word } \times 32 \text{ simple-match } \times \text{char list } \times \text{simple-action}) \text{list} \) to an OpenFlow table. While converting the \( \text{char list } \times \text{simple-action} \) tuple is straightforward, converting the \( \text{simple-match} \) to an equivalent list of \( \text{of-match-field set} \) is non-trivial. This is done by the function \( \text{simple-match-to-of-match} \).

The main difficulties for \( \text{simple-match-to-of-match} \) lie in making sure that the prerequisites are satisfied and in the fact that a \( \text{simple-match} \) operates on slightly stronger match expressions.

- A \( \text{simple-match} \) allows a (string) prefix match on the input and output interfaces. Given a list of existing interfaces on the router \( \text{ifs} \), the function has to insert flow entries for each interface matching the prefix.
- A \( \text{simple-match} \) can match ports by an interval. Now it becomes obvious why Section 1.2.1 added bitmasks to \( L_4\text{Src} \) and \( L_4\text{Dst} \). Using the algorithm to split word intervals into intervals that can be represented by prefix matches from [6], we can efficiently represent the original interval by a few (32 in the worst case) prefix matches and insert flow entries for each of them.

The following lemma characterizes \( \text{simple-match-to-of-match} \):

Lemma \( \text{simple-match-to-of-match} \):

assumes \( \text{simple-match-valid} \text{r} \text{p-iface} p \in \text{set ifs} \text{match-iface (oiface r) (p-oiface p)} \text{p-l2type p = 0x800} \)

shows \( \text{simple-matches r p (exists gr set (simple-match-to-of-match r ifs)) OF-match-fields gr p = Some True} \)

using \( \text{assms simple-match-to-of-matchD simple-match-to-of-matchI by blast} \)

The assumptions are to be read as follows:

\(^9\text{It might be possible to represent the interval match more efficiently than a split into prefixes. However, that would produce overlapping matches (which is not a problem if we assign separate priorities) and we did not have a verified implementation of an algorithm that does so.}\)
Lemma \( \text{lr-of-tran} \ rt \ fw \ ifs \equiv \)
if \( \neg \) (no-oif-match \( fw \) \( \land \) has-default-policy \( fw \) \( \land \) simple-fw-valid \( fw \) \( \land \) valid-prefixes \( rt \) \( \land \) has-default-route \( rt \) \( \land \) distinct \( ifs \))
then Inl "Error in creating OpenFlow table: prerequisites not satisfied"
else (let
nfw = map simple-rule-dtor \( fw \);
frt = map (\( \lambda \) r. (route2match r, output-iface (routing-action r))) \( rt \);
nrd = generalized-fw-join frt \( nfw \);
ard = (map (apfst of-nat) \( \circ \) annotate-rlen) \( nrd \)
in
if length \( nrd \) < unat (max-word :: 16 word)
then Inr \( \text{pack-OF-entries} \ ifs \ ard \)
else Inl "Error in creating OpenFlow table: priority number space exhausted"
)

Unfolding Let-def \( \text{lr-of-tran-def} \) \( \text{lr-of-tran-fbs-def} \) \( \text{lr-of-tran-s1-def} \) comp-def route2match-def by force

Figure 1: Function for translating a 'i simple-rule list, a 'i routing-rule list, and a list of interfaces to a flow table.

- The match \( r \) has to be valid, i.e. it has to use valid-prefix matches, and it cannot use anything other than 0-65535 for the port matches unless its protocol match ensures TCP, UDP or L4-Protocol.SCTP.

- simple-match-to-of-match cannot produce rules for packets that have input interfaces that are not named in the interface list.

- The output interface of \( p \) has to match the output interface match of \( r \). This is a weakened formulation of ofiface \( r = \text{ifaceAny} \), since

\[
\text{match-iface} \ \text{ifaceAny} \ i
\]

We require this because OpenFlow field matches cannot be used to match on the output port — they are supposed to match a packet and decide an output port.

- The simple-match type was designed for IP(v4) packets, we limit ourselves to them.

The conclusion then states that the simple-match \( r \) matches iff an element of the result of simple-match-to-of-match matches. The third assumption is part of the explanation why we did not use simple-linux-router-altered: simple-match-to-of-match cannot deal with output interface matches. Thus, before passing a generalized simple firewall to \( \text{pack-OF-entries} \), we would have to set the output ports to ifaceAny. A system replace output interface matches with destination IP addresses has already been formalized and will be published in a future version of [5]. For now, we limit ourselves to firewalls that do not do output port matching, i.e., we require \( \neg \)no-oif-match \( fw \).

Given discussed properties, we present the central theorem for our translation in Figure 2. The first two assumptions are limitations on the traffic we make a statement about. Obviously, we will never see any packets with an input interface that is not in the interface list. Furthermore, we do not state anything about non-IPv4 traffic. (The traffic will remain unmatched in the flow table, but we have not verified that.) The last assumption is that the translation does not return a run-time error. The translation will return a run-time error if the rules cannot be assigned priorities from a 16 bit integer, or when one of the following conditions on the input data is not satisfied:

Lemma
\[
\neg \text{no-oif-match} \fw \lor
\neg \text{has-default-policy} \fw \lor
\neg \text{simple-fw-valid} \fw \lor
\neg \text{valid-prefixes} \ rt \lor
\neg \text{has-default-route} \ rt \lor
\neg \text{distinct} \ ifs \implies
\]
Theorem

fixes
\( p :: (32, 'a) \) simple-packet-ext-scheme

assumes
\( \text{p-iiface p} \in \text{set ifs and p-l2type p} = 0x800 \)
\( \text{lr-of-tran rt fw ifs} = \text{Inr oft} \)

shows
\( \text{OF-priority-match OF-match-fields-safe oft p} = \text{Action [Forward oif]} \leftrightarrow \text{simple-linux-router-nol12 rt fw p} = \) (Some (p[p-\text{ofiface} := \text{oif}]))
\( \text{OF-priority-match OF-match-fields-safe oft p} = \text{Action []} \leftrightarrow \text{simple-linux-router-nol12 rt fw p} = \text{None} \)
\( \text{OF-priority-match OF-match-fields-safe oft p} \neq \text{NoAction} \)
\( \text{OF-priority-match OF-match-fields-safe oft p} \neq \text{Undefined} \)
\( \text{OF-priority-match OF-match-fields-safe oft p} \neq \text{Action ls} \)
\( \exists \text{ls. length ls} \leq 1 \wedge \text{OF-priority-match OF-match-fields-safe oft p} \neq \text{Undefined} \)

using assms lr-of-tran-correct by simp-all

∃ err. lr-of-tran rt fw ifs = Inl err unfolding lr-of-tran-def by(simp split: if-splits)

1.3.3 Comparison to Exodus

We are not the first researchers to attempt automated static migration to SDN. The (only) other attempt we are aware of is Exodus by Nelson et al. [10].

There are some fundamental differences between Exodus and our work:

- Exodus focuses on Cisco IOS instead of Linux.
- Exodus is not limited to using a single flow table.
- Exodus requires continuous controller interaction for some of its functions.
- Exodus attempts to support as much functionality as possible and has implemented support for dynamic routing, VLANs and NAT.
- Nelson et al. reject the idea that the translation could or should be proven correct.

2 Evaluation

In Section 1, we have made lots of definitions and created lots of models. How far these models are in accordance with the real world has been up to the vigilance of the reader. This section attempts to alleviate this burden by providing some examples.

2.1 Mininet Examples

The first example is designed to be minimal while still showing the most important properties of our conversion. For this purpose, we used a Linux firewall F, that we want to convert. We gave it two interfaces, and connected one client each. Its original configuration and the ruleset resulting from the translation is shown in Figure 3. (The list of interfaces can be extracted from the routing table; s1-lan received port number 1.) While the configuration does not fulfill any special function (especially, no traffic from the interface s1-wan is permitted), it is small enough to let us have a detailed look. More specifically, we can see how the only firewall rule (Line 2) got combined with the first rule of the routing table to form Line 1 of the OpenFlow rules. This also shows why the bitmasks on the layer 4 ports are necessary. If we only allowed exact matches, we would have \(2^{15}\) rules instead of just one. Line 2 of the OpenFlow ruleset has been formed by combining the default drop policy with Line 1 of the routing table.
In a similar fashion, Line 2 of the routing rules has also been combined with the two firewall rules. However, as 10.0.2.0/24 from the firewall and 10.0.1.0/24 from the routing table have no common elements, no rule results from combining Line 2 and Line 2. In a similar fashion, the rest of the OpenFlow ruleset can be explained.

We feel that it is also worth noting again that it is necessary to change the IP configuration of the two devices attached to F. Assuming they are currently configured with, e.g., 10.10.100/24 and 10.0.2.1/24, the subnet would have to be changed from 24 to 22 or lower to ensure that a common subnet is formed and the MAC layer can function properly.

Next, we show a somewhat more evolved example. Its topology is depicted in Figure 4a. As before, we called the device to be replaced F. It is supposed to implement the simple policy that the clients H1 and H2 are allowed to communicate with the outside world via HTTP, ICMP is generally allowed, any other traffic is to be dropped (we neglected DNS for this example). We used the iptables configuration that is shown in Figure 4b. The routing table is the same as in the first example network.

The topology has been chosen for a number of reasons: we wanted one device which is not inside a common subnet with F and thus requires no reconfiguration for the translation. Moreover, we wanted two devices in a network that can communicate with each other while being overheard by F. For this purpose, we added two clients H1 and H2 instead of just one. We connected them with a broadcasting device.\textsuperscript{10}

Executing our conversion function results in 36 rules,\textsuperscript{11} we decided not to include them here. Comparing to the first example network, the size of the ruleset seems relatively high. This can be explained by the port matches: 1024-65535 has to be expressed by 6 different matches, $tp_{src}=1024/0xffff$, $tp_{src}=2048/0xf800$, \ldots, $tp_{src}=32768/0x8000$ (or $tp_{dst}$ respectively).

When installing these rules, we also have to move all of H1, H2 and S1 into a common subnet. We chose 10.0.0.0/16 and updated the IP configuration of the three hosts accordingly. As discussed, the configuration of S2 did not have to be updated, as it does not share any subnet with F. We then tested reachability for TCP 22 and 80 and ICMP. The connectivity between all pairs of hosts (H1,H2,S1 and S2) remained the same compared to before the conversion. This shows that the concept can be made to work.

However, the example also reveals a flaw: When substituting the more complete model of a linux firewall with the simple one in Section 1.1, we assumed that the check whether the correct MAC address is set and the packets are destined for the modelled device would never fail — we assumed that all traffic arriving at a device is ac-

\textsuperscript{10}For the lack of a hub in mininet, we emulated one with an OpenFlow switch.

\textsuperscript{11}If we had implemented some spoofing protection by adding $-s 10.0.1.0/24$ to the respective rule, the number of rules would have been increased to 312. This is because a cross product of two prefix splits would occur.

53
F

S1

H1

(a) Topology

S2

H2

(b) FORWARD chain

Figure 4: Example Network 2

1. :FORWARD DROP [0:0]
2. -A FORWARD -p icmp -j ACCEPT
3. -A FORWARD -i s1-lan -p tcp -m tcp --sport 1024:65535 --dport 80 -j ACCEPT
4. -A FORWARD -d 10.0.1.0/24 -i s1-van -p tcp -m tcp --sport 80 --dport 1024:65535 -j ACCEPT

2.2 Performance Evaluation

Unfortunately, we do not have any real-world data that does not use output port matches as required in Section 1.3. There is thus no way to run the translation on the real-world firewall rulesets we have available and obtain a meaningful result. Nevertheless, we can use a real-world ruleset to evaluate the performance of our translation. For this purpose, we picked the largest firewall from the firewall collection from [6]. A significant amount of time is necessary to convert its FORWARD chain including 4946 rules\textsuperscript{12} to the required simplified firewall form. Additionally to the simplified firewall, we acquired the routing table (26 entries) from the same machine. We then evaluated the time necessary to complete the translation and the size of the resulting ruleset when using only the first $n$ simple firewall rules and the full routing table. The result is shown in Figure 5. Given the time necessary to complete the conversion of the iptables firewall to a simple firewall, it is reasonable to say that the translation function is efficient enough. At first glance, size of the resulting ruleset seems high. This can be explained by two facts:

- The firewall contains a large number of rules with port matches that allow the ports 1-65535, which requires 16 OpenFlow rules.

\textsuperscript{12}In the pre-parsed and already normalized version we used for this benchmark, it took 45s. The full required time lies closer to 11min as stated in [6].

Figure 5: Benchmark
• Some combinations of matches from the firewall and the routing table cannot be ruled out, since the firewall match might only contain an output port and the rule can thus only apply for the packets matching a few routing table entries. However, the translation is not aware of that and can thus not remove the combination of the firewall rule and other routing table entries.

In some rules, the conditions above coincide, resulting in 416 (= 16 \cdot 26) rules. To avoid the high number of rules resulting from the port matches, rules that forbids packets with source or destination port 0 could be added to the start of the firewall and the 1-65535 could be removed; dealing with the firewall / routing table problem is part of the future work on output interfaces.

3 Conclusion and Future Work

We believe that we have shown that it is possible to translate at least basic configurations of a linux firewall into OpenFlow rulesets while preserving the most important aspects of the behavior. We recognize that our system has limited practical applicability. One possible example would be a router or firewall inside a company network whose state tables have been polluted by special attack traffic. Our translation could provide an OpenFlow based stateless replacement. However, given the current prerequisites the implementation has on the configuration, this application is relatively unlikely.

For the configuration translation, we have contributed formal models of a linux firewall and of an OpenFlow switch. Furthermore, the function that joins two firewalls and the function that translates a simplified match from [6] to a list of equivalent OpenFlow field match sets are contributions that we think are likely to be of further use.

We want to explicitly formulate the following two goals for our future work:

• We want to deal with output interface matches. The idea is to formulate and verify a destination interface / destination IP address rewriting that can exchange output interfaces and destination IP addressed in a firewall, based on the information from the routing table.\footnote{As of now this has already been implemented, but is not yet fully ready.}

• We want to develop a system that can provide a stricter approximation of stateful matches so our translation will be applicable in more cases.

References


