Explainable Network Verification via Subspecifications

User Study - Introduction of Background Knowledge

Background: Explainable Network Verification

Network verifiers often give YES/NO (with a counterexample) answers, without explaining ***why***.

Example: suppose we want a BGP policy blocking the private prefix `192.168.0.0/16`.

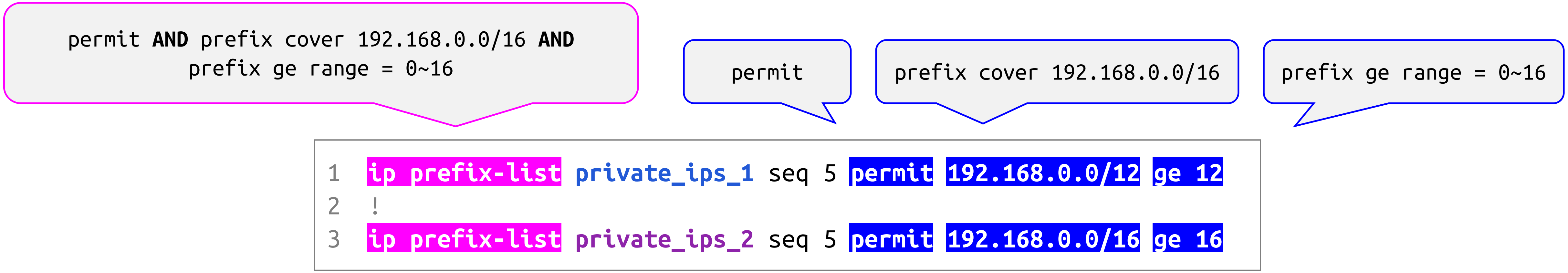
```
ip prefix-list private_ips_1 seq 5 permit 192.168.0.0/12 ge 12
!
ip prefix-list private_ips_2 seq 5 permit 192.168.0.0/16 ge 16
```

Both of them pass the verification.

However, **`private_ips_2`** is more *precise* than **`private_ips_1`**.
Overly restrictive filter may block more prefix than necessary.

Explainable Network Verification

Why a specific field, line, or block of the configuration satisfies the specification?



permit **AND** prefix cover 192.168.0.0/16 **AND** prefix ge range = 0~16

permit

prefix cover 192.168.0.0/16

prefix ge range = 0~16

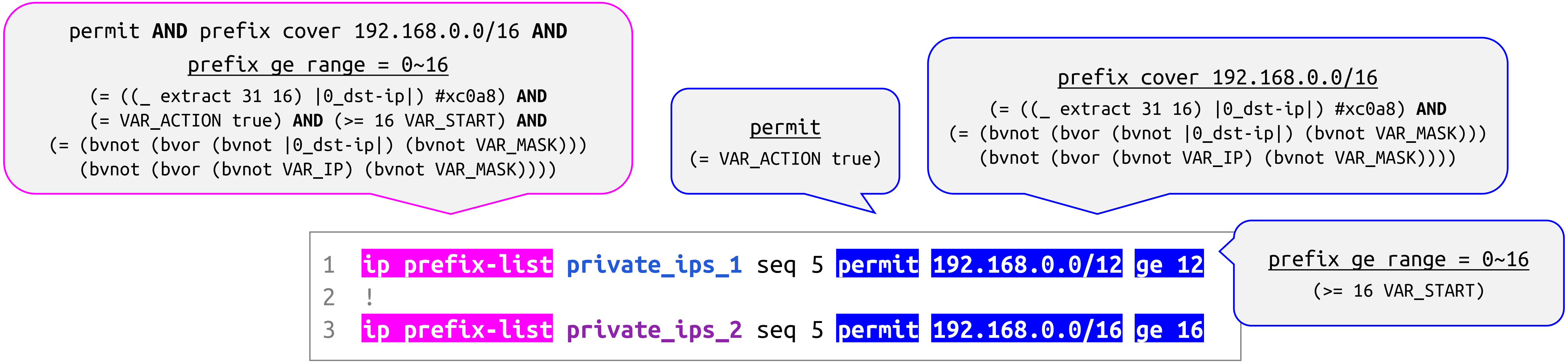
```
ip prefix-list private_ips_1 seq 5 permit 192.168.0.0/12 ge 12
!
ip prefix-list private_ips_2 seq 5 permit 192.168.0.0/16 ge 16
```

Both of them pass the verification.

`private_ips_2` is the more precise option.

Explainable Network Verification via Subspecifications

Localized Subspecifications (Subspecs): **the safe modification scope** of that field, line, or block, while preserving the prior verification success.



permit **AND** prefix cover 192.168.0.0/16 **AND**

prefix ge range = 0~16

(= ((_ extract 31 16) |0_dst-ip|) #xc0a8) **AND**
(= VAR_ACTION true) **AND** (>= 16 VAR_START) **AND**
(= (bvnot (bvor (bvnot |0_dst-ip|) (bvnot VAR_MASK)))
(bvnot (bvor (bvnot VAR_IP) (bvnot VAR_MASK))))

permit

(= VAR_ACTION true)

prefix cover 192.168.0.0/16

(= ((_ extract 31 16) |0_dst-ip|) #xc0a8) **AND**
(= (bvnot (bvor (bvnot |0_dst-ip|) (bvnot VAR_MASK)))
(bvnot (bvor (bvnot VAR_IP) (bvnot VAR_MASK))))

```
ip prefix-list private_ips_1 seq 5 permit 192.168.0.0/12 ge 12
!
ip prefix-list private_ips_2 seq 5 permit 192.168.0.0/16 ge 16
```

prefix ge range = 0~16

(>= 16 VAR_START)

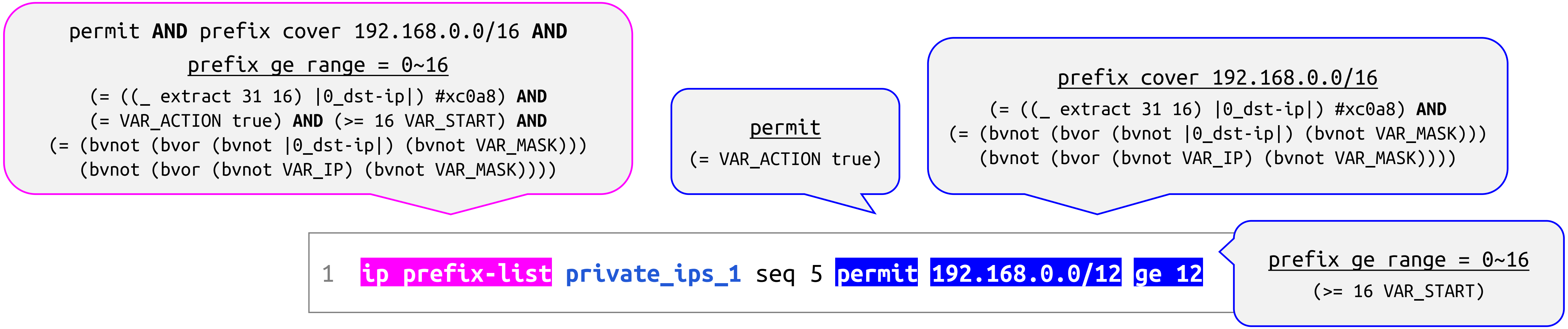
Tips for Subspecs

1. modifications ***satisfying*** the subspec bounds are guaranteed to preserve the verified specifications

```
ip prefix-list private_ips_1 seq 5 permit 192.168.0.0/16 ge 16
```

2. modifications ***exceeding*** the subspec bounds **may violate** the verified specifications ***(sound but not complete)***

```
ip prefix-list private_ips_1 seq 5 deny 192.168.0.0/17 ge 17
```



```
permit AND prefix cover 192.168.0.0/16 AND
prefix ge range = 0~16
(= ((_ extract 31 16) |0_dst-ip|) #xc0a8) AND
(= VAR_ACTION true) AND (>= 16 VAR_START) AND
(= (bvnot (bvor (bvnot |0_dst-ip|) (bvnot VAR_MASK)))
(bvnot (bvor (bvnot VAR_IP) (bvnot VAR_MASK))))
```

```
permit
(= VAR_ACTION true)
```

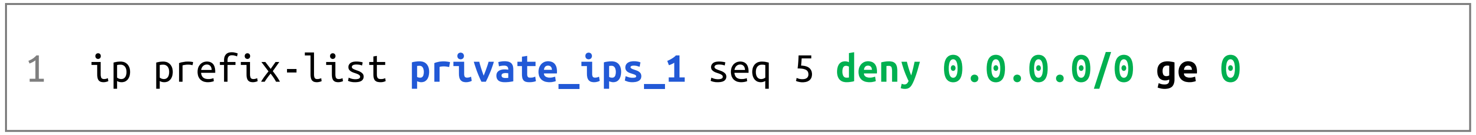
```
prefix cover 192.168.0.0/16
(= ((_ extract 31 16) |0_dst-ip|) #xc0a8) AND
(= (bvnot (bvor (bvnot |0_dst-ip|) (bvnot VAR_MASK)))
(bvnot (bvor (bvnot VAR_IP) (bvnot VAR_MASK))))
```

```
ip prefix-list private_ips_1 seq 5 permit 192.168.0.0/12 ge 12
```

```
prefix ge range = 0~16
(>= 16 VAR_START)
```

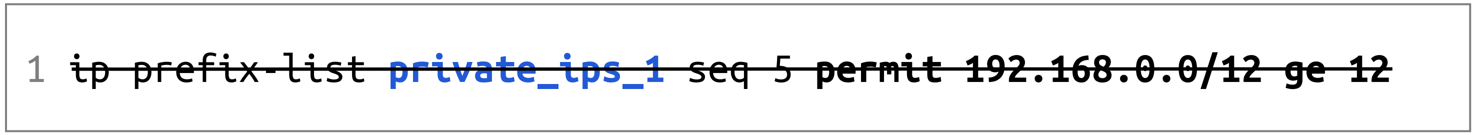
Tips for Empty Subspecs

1. ***safely modify*** that field with **empty subspec** without breaking the verified specifications

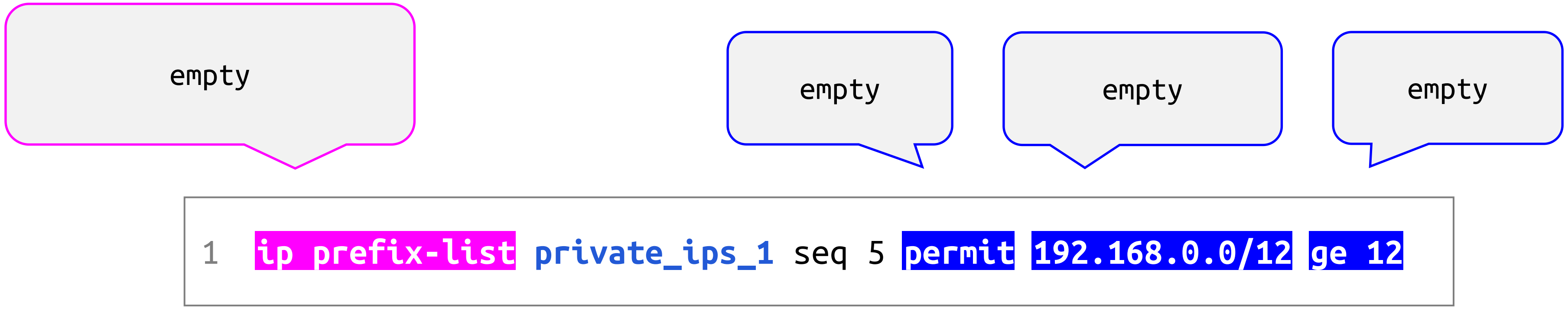


```
ip prefix-list private_ips_1 seq 5 deny 0.0.0.0/0 ge 0
```

2. ***safely remove*** that line with **empty line-level subspec** without breaking the verified specifications (or a line contains **only a single field-level subspec** and the field-level subspec is **empty**)



~~ip prefix-list private_ips_1 seq 5 permit 192.168.0.0/12 ge 12~~



```
ip prefix-list private_ips_1 seq 5 permit 192.168.0.0/12 ge 12
```

Tips for User Study

1. In this user study, we consider two granularities: **field-level** and **line-level** subspecs.

2. In this user study, the eBGP route selection process only involves **AS-path length**.

3. In this user study, the route-map naming rule is **Router_Direction(IN_FROM/OUT_TO)_Peer**.

Explainable Network Verification via Subspecifications

User Study - Introduction of Background Knowledge

Thank you for participating in this user study !