A General Approach for Network Configurations Update Verification

Configuring a network is always hard and error-prone. We propose NUV, a framework for network configuration update verification. It outputs verification queries for the endpoints whose forwarding behavior changes with updated network configuration.

In this report, we now provide some of the research results, as there is an paper being submitted.

Theorem 1: Suppose we have well-formed $\mathcal{N}_d^s$, $\mathcal{S}|\mathcal{N}_d^s$. For any λ, there exists equivalence solution $\lambda^{'}$ and vice-versa.

Proof: ($\Rightarrow$) Given solution λ to $\mathcal{N}_d^s$, we show that removing ports which are not in the path p, solution λ will not be impacted. For solution λ, there exists a path $p^{'} = node(s), v_1, v_2, v_3, ..., v_i, ..., node(d)$ where $p^{'} \in fwd_\lambda(d)$. The label of the path is $\lambda(node(s)), \lambda(v_1), \lambda(v_2), \lambda(v_3), ...,$ $\lambda(v_i), ..., \lambda\ (node(d))$. Suppose solution λ is impacted, then we know that there exists $\lambda(v_i)$, $v_i \notin p$ in the solution. Consider an arbitrary such v_i. By the definitions of λ and $choices_\lambda$, we have that there exists $v_i.i$, $v_i.i \in fwd_\beta(v^{'})$. With the definitions of fwd_β and $choices_\beta$, we know that there exists $\lambda(v^{'}.i^{'})$, $v^{'}.i^{'} = \gamma(v_i.i)$. By the transitivity of link connection, we have that solution λ forwards along a path $s, ...,\ v_i.i, v^{'}.i^{'},\ ..., d$. Considering loop-free and non-spontaneous properties of network instance, the path must be of one the loop-free paths from destination d to source s. This leads to a contradiction with the fact that there exist some nodes in the solution λ are not in p, and hence, solution λ will not be impacted. Therefore, we have that there exists an equivalent solution $\lambda^{'}$ of $\mathcal{S}|\mathcal{N}_d^s$ with solution λ.

($\Leftarrow$) We are given a solution $\lambda^{'}$ of $\mathcal{S}|\mathcal{N}_d^s$ and show that there exists λ in $\mathcal{N}_d^s$. Suppose $\lambda^{'}$ is $\lambda^{'}(v_1), \lambda^{'}(v_2), \lambda^{'}(v_3), ...,$ $\lambda^{'}(v_i), ...,\ \lambda^{'}(v_n)$, where $v_1 = node(s)$ and $v_n = node(d)$. Then, we show that adding some ports or links which are in path p, the solution $\lambda^{'}$ of $\mathcal{S}|\mathcal{N}_d^s$ will not be impacted. Suppose the solution $\lambda^{'}$ is impacted, then we know that $\exists\lambda^{''}(v_i)$, $v_i \notin p$ in the solution $\lambda^{''}$. Consider an arbitrary such v_i. By the definitions of $\lambda^{''}$ and $choices_{\lambda^{''}}$, we get $\exists v_i.i$, $v_i.i \in fwd_\beta(v^{'})$. With the definitions of fwd_β and $choices_\beta$, we know that $\exists\lambda^{''}(v^{'}.i^{'})$, $v^{'}.i^{'} = \gamma(v_i.i)$. By the transitivity of link connection, we have that solution $\lambda^{''}$ forwards along a path $s, ...,\ v_i.i, v^{'}.i^{'},\ ..., d$. Considering loop-free and non-spontaneous properties of network instance, the path must be one of the loop-free paths. This leads to a contradiction with the fact that there exist some nodes in the solution $\lambda^{''}$ are not in the path p. Therefore, $\lambda^{''}$ does not exist. Therefore the solution $\lambda^{'}$ of $\mathcal{N}_d^s$ will not be impacted. Considering the definition of $\mathcal{S}|\mathcal{N}_d^s$ and $\mathcal{N}_d^s$, we have that there exists an equivalence solution λ with solution $\lambda^{'}$.

Corollary 1: Suppose we have well-formed $\mathcal{N}_d^s$, $\mathcal{N}^{'s}_{\ d}$ is obtained by pruning $\mathcal{N}_d^s$ (i.e., removing some of the ports that are not in $\mathcal{S}|\mathcal{N}_d^s$), for any solution $\lambda^{'}$ of $\mathcal{N}^{'s}_{\ d}$, there exists equivalent λ of $\mathcal{N}_d^s$.

Proof: For network instance $\mathcal{N}_d^s$ and its sub-instance $\mathcal{S}|\mathcal{N}_d^s$, by Theorem 1, we know there exist solutions λ and $\overline{\lambda}$ are label-equivalence. We get that $\forall v.i.\ \lambda(v.i) = \overline{\lambda}(v.i)$. For network instance $\mathcal{N}^{'s}_{\ d}$, and its sub-instance $\mathcal{S}|\mathcal{N}'^s_d$, we have that there exist solutions λ' and $\overline{\lambda'}$ are label-equivalence, we $\forall v.i.\ \lambda'(v.i) = \widehat{\lambda'}(v.i)$. The sub-instance of $\mathcal{N}^{'s}_{\ d}$ is also $\mathcal{S}|\mathcal{N}_d^s$, because it is obtained by removing some of the ports of $\mathcal{N}_d^s$ are not involved in $\mathcal{S}|\mathcal{N}_d^s$. The sub-instances of $\mathcal{N}_d^s$ and $\mathcal{N}^{'s}_{\ d}$ are the same, $\forall v.i.\ \overline{\lambda}(v.i) = \widehat{\lambda'}(v.i)$. By transitivity, we have $\forall v.i.\ \lambda(v.i) = \widehat{\lambda'}(v.i)$.

Lemma 1: Suppose we have well formed network instance $\mathcal{N}_d^s, \overline{\mathcal{N}_d^s}$ and an effective abstraction that is data plane choice-equivalence, then the abstraction is label-equivalence.

Proof: Looking at the definition of λ , there are two cases to consider. First, we observe that if $v.i = s$, then $\lambda(s) = a_s$. It follows that $\overline{\lambda}(f(s)) = \overline{\lambda}(\overline{s}) = \overline{a_s} = h(a_s)) = h(\lambda(s))$. For the second cases, we show the implications separately.

Case ($\Rightarrow$) Assume $\lambda(v) = a$. By the definition of λ, we know that there are some links such that $(a, v.i, v.i^{'}) \in choices_\lambda(v)$. Consider all concrete links $(a, v.i, v.i^{'}) \in choices_\lambda(v)$. From choice-equivalence, we know that $(h(a), f(v.i), f(v.i^{'})) \in \underline{choices_\lambda(f(v))}$ for each such pair. By the definition of λ, we then know that $\overline{\lambda}(f(v)) = A = h(a)$. By transitivity, $\forall v.i.\ h(\lambda(v.i)) = \overline{\lambda}(f(v.i))$.

Case ($\Leftarrow$) Assume $\overline{\lambda}(f(v)) = \underline{A}$. We know that $A \in choices_\lambda(f(v))$. Assume $(A, \overline{v.i}, \overline{v.i^{'}}) \in choices_\lambda(f(v))$. Consider all such $(A, \overline{v.i}, \overline{v.i^{'}}) \in choices_\lambda(f(v))$. From choice-equivalence, we know that for any concrete $v.i$ that $f(v.i) = \overline{v.i}$, there exists a such that $h(a) = A$ and $(a, v.i, v.i^{'}) \in choices_\lambda(v)$. Therefore, $a \in choices_\lambda(v)$. Finally, we obtain that the labeling can be a $(\lambda(v) = a)$. It follows from transitivity that $h(\lambda(v)) = \overline{\lambda}(f(v))$.

Lemma 2: Suppose we have well formed network instance $\mathcal{N}_d^s$ and $\overline{\mathcal{N}_d^s}$ and a effective abstraction that is data plane choice-equivalence, then the abstraction is fwd-equivalence.

Case ($\Rightarrow$) We assume $(v.i, v.i^{'}) \in fwd_\lambda(v)$, and need to show that $(f(v.i), f(v.i^{'})) \in \overline{fwd}_{\overline{\lambda}}(f(v))$. By the definition of fwd_λ, we know that $\exists a.(a, v.i, v.i^{'}) \in choices_\lambda(v)$. From choice-equivalence, this means that $(h(a), f(v.i), f(v.i^{'})) \in \overline{choices}_\lambda(f(v))$. Because we have label-equivalence, and recall from label equivalence: $h(\lambda(v)) = \overline{\lambda}(f(v))$. By the definition of $\overline{fwd}_{\overline{\lambda}}$: $(f(v.i), f(v.i')) \in \overline{fwd}_{\overline{\lambda}}(f(v))$.

Case ($\Leftarrow$) We will assume $(\overline{v.i}, \overline{v.i'}) \in fwd_{\lambda}(\overline{v})$ and show that there exists a $v.i'$ such that $(v.i, v.') \in fwd_{\lambda}(v)$. By the definition of fwd_{λ}, we know that $\exists A.(A, \overline{v.i}, \overline{v.'}) \in \overline{choices}_{\lambda}(\overline{v})$. From choice-equivalence, this means $\forall \overline{v.i} = f(v.i), \exists a.h(a) = A \wedge (a, v.i, v.i') \in choices_{\lambda}(v)$. Consider any such $(v.i, v.i')$ where $f(v.i, v.i') = (\overline{v.i}, \overline{v.i'})$. Rewriting slightly, we get $a.(a, v.i, v.i') \in choices_{\lambda}(v) \wedge \overline{\lambda}(f(v)) \approx h(a)$. From transfer-equivalence, we know that $\overline{\lambda}(f(v)) = h(\lambda(v))$ and so $h(a) \approx h(\lambda(v))$, and therefore $a \approx \lambda(v)$. Finally, from the definition of fwd_{λ}, we have $(v.i, v.i') \in fwd_{\lambda}(v)$.

Theorem 2: There is a solution λ to well-formed network instance $\mathcal{N}_d^s$ iff there is a solution $\overline{\lambda}$ to it effective abstract network instance $\overline{\mathcal{N}}_d^s$, and solution λ and $\overline{\lambda}$ are label-equivalence.

Proof: By the definition of λ, there are two cases to consider. First, we observe that if $v.i = s$, then $\lambda(s) = a_s$. It follows that $\overline{\lambda}(f(s)) = \overline{\lambda}(\overline{s}) = \overline{a_s} = h(a_s)) = h(\lambda(s))$. For the second case, we show the implications separately.

($\Rightarrow$) We are given solution λ, and show that there exists a label-equivalence solution $\overline{\lambda}$. By acl-equivalence, we know that $\overline{\eta}(f(v.i), h(\lambda(v))) = h\ (\eta(v.i,\ \lambda(v))) = h(a)$. By transitivity and label-equivalence (IH), then we get that $\overline{\eta}(f(v.i),\ \overline{\lambda}\ (f(v)))) = h(a)$. By the lemma from [1], we have that there is a solution β to $\mathcal{N}_d^s$ iff there is a solution $\overline{\beta}$ to $\overline{\mathcal{N}}_d^s$, and β and $\overline{\beta}$ are control plane label-equivalence and fwd-equivalence. Hence, we get that $\forall v.i, v'.i', (v.i, v'.i') \in fwd_{\beta}(v) \Leftrightarrow (\overline{v.i}, \overline{v'.i'}) \in \overline{fwd}_{\overline{\beta}}(f(v))$. By the definition of $choice_{\lambda}$, we have that $(h(a), f(v.i), f(v.i')) \in \overline{choice}_{\overline{\lambda}}(f(v))$. Therefore, we have data plane choice-equivalence. With Lemma 2, it follows that we have solution λ and $\overline{\lambda}$ are label-equivalence and fwd-equivalence.

($\Leftarrow$) Given solution $\overline{\lambda}$, we show that there exists a label-equivalence solution λ. Consider an arbitrary $\overline{v.i}$. Suppose $(A, \overline{v.i}, \overline{v.i'}) \in \overline{choice}_{\lambda}(\overline{v})$. From $\forall\exists$ abstraction, we know that there must be at least some $(v.i,\ v.i')$ such that $f(v.i, v.i') = (\overline{v.i},\ \overline{v.i'})$. Consider arbitrary such $(v.i, v.i')$. We know that $A = \overline{\eta}(f(v.i),\ \overline{\lambda}(f(v))))$. By the IH, we have $\overline{\lambda}(f(v)) = h(\lambda(v))$. Therefore, $A = \overline{\eta}(f(v.i), h(\lambda(v))) = h\ (\eta(v.i, \lambda(v)))$. Let a stand for $\eta(v.i, \lambda(v))$. Then $\eta(v.i, \lambda(v)) = a$ and $h(a) = A$. By the definition of $choice_{\lambda}$, it follows that $\exists a, h(a) = A \wedge (a, v.i, v.i' \in choice_{\lambda}(v)$. With Lemma 2, This implies that we also have label-equivalence and fwd-equivalence.

Corollary 2: Suppose we have well-formed $\mathcal{N}_d^s$, $\overline{\mathcal{N}}_d^s$ and $\widehat{\mathcal{N}}_d^s$ and $\overline{\widehat{\mathcal{N}}}_d^s$ with effective abstractions (f, h) and $(\widehat{f}, \widehat{h})$, respectively. if $\overline{\mathcal{N}}_d^s$ equals $\overline{\widehat{\mathcal{N}}}_d^s$, for any λ there exists label and fwd-equivalence $\widehat{\lambda}$ and vice-versa.

Proof: (i) Suppose λ is a solution for $\mathcal{N}_d^s$. From theorem 2, we know that there exists a solution $\overline{\lambda}$ for $\overline{\mathcal{N}}_d^s$, λ and $\overline{\lambda}$ are fwd-equivalence. Looking at the definition of label and fwd-equivalence, we have $\forall v.i.\ h(\lambda(v.i)) = \overline{\lambda}(f(v.i))$ and $\forall v.i, v'.i'.\ (v.i, v'.i') \in fwd_{\lambda}(v) \Leftrightarrow (\overline{v.i}, \overline{v'.i'}) \in \overline{fwd}_{\overline{\lambda}}(\overline{v})$. Similarly, for $\widehat{\mathcal{N}}_d^s$ and $\overline{\widehat{\mathcal{N}}}_d^s$, we have $\forall \widehat{v.i}.\ \widehat{h}(\widehat{\lambda}(\widehat{v.i})) = \overline{\widehat{\lambda}}(\widehat{f}(\widehat{v.i}))$ and $\forall \widehat{v.i}, \widehat{v'.i'}.\ (\widehat{v.i}, \widehat{v'.i'}) \in fwd_{\widehat{\lambda}}(\widehat{v}) \Leftrightarrow (\overline{\widehat{v.i}}, \overline{\widehat{v'.i'}}) \in \overline{\widehat{fwd}}_{\overline{\widehat{\lambda}}}(\overline{\widehat{v}})$. (ii) As $\overline{\mathcal{N}}_d^s$ equals $\overline{\widehat{\mathcal{N}}}_d^s$, we know that $\forall v.i.\ \overline{\lambda}(f(v.i)) = \overline{\widehat{\lambda}}(\widehat{f}(\widehat{v.i}))$ and $\forall v.i, v'.i'.\ (\overline{v.i}, \overline{v'.i'}) \in \overline{fwd}_{\overline{\lambda}}(\overline{v}) \Leftrightarrow (\overline{\widehat{v.i}}, \overline{\widehat{v'.i'}}) \in \overline{\widehat{fwd}}_{\overline{\widehat{\lambda}}}(\overline{\widehat{v}})$. By transitivity, we have label-equivalence $\forall v.i.\ h(\lambda(v.i)) = \widehat{\lambda}(f(v.i))$ and fwd-equivalence $\forall v.i, v'.i'.\ (v.i, v'.i') \in fwd_{\lambda}(v) \Leftrightarrow \widehat{v.i}, \widehat{v'.i'} \in \widehat{fwd}_{\widehat{\lambda}}(\widehat{v})$

Corollary 3: Suppose we have well-formed $\mathcal{N}_d^s$, $\overline{\mathcal{N}}_d^s$ and $\widehat{\mathcal{N}}_d^s$ and $\overline{\widehat{\mathcal{N}}}_d^s$ with effective abstractions (f, h) and $(\widehat{f}, \widehat{h})$, respectively. If $\overline{\mathcal{S}|\mathcal{N}}_d^s$ equals $\overline{\widehat{\mathcal{S}|\mathcal{N}}}_d^s$, for any λ, there exists label and fwd-equivalence $\widehat{\lambda}$ and vice-versa.

Proof: (i) Suppose λ is a solution for $\mathcal{N}_d^s$. From Theorem 2, we know there exist solutions λ and $\overline{\lambda}$ are fwd-equivalence. Also $\forall v.i.\ h(\lambda(v.i)) = \overline{\lambda}(f(v.i))$ and $\forall v.i, v'.i'.\ (v.i, v'.i') \in fwd_{\lambda}(v) \Leftrightarrow (\overline{v.i}, \overline{v'.i'}) \in \overline{fwd}_{\overline{\lambda}}(\overline{v})$. From Theorem 1 we know that we have $\forall v.i.\ \overline{\lambda}(f(v.i)) = \overline{\lambda}(f_{S|N}(v.i))$ and $\forall v.i, v'.i'.\ (\overline{v.i}, \overline{v'.i'}) \in \overline{fwd}_{\overline{\lambda}}(\overline{v}) \Leftrightarrow (\overline{v.i}, \overline{v'.i'}) \in \overline{fwd_{S|N}}_{\overline{\lambda_{S|N}}}(\overline{v})$. Thus $\forall v.i.\ h(\lambda(v.i)) = \overline{\lambda}(f_{S|N}(v.i))$ and $\forall v.i, v'.i'.\ (v.i, v'.i') \in fwd_{\lambda}(v) \Leftrightarrow (\overline{v.i}, \overline{v'.i'}) \in \overline{fwd_{S|N}}_{\overline{\lambda_{S|N}}}(\overline{v})$. Similarly, for $\widehat{\mathcal{N}}_d^s$ and $\overline{\widehat{\mathcal{N}}}_d^s$. By transitivity, we have label-equivalence and fwd-equivalence.

References

[1] R. Beckett, A. Gupta, R. Mahajan, and D. Walker, "Control plane compression," in *ACM SIGCOMM*, 2018.