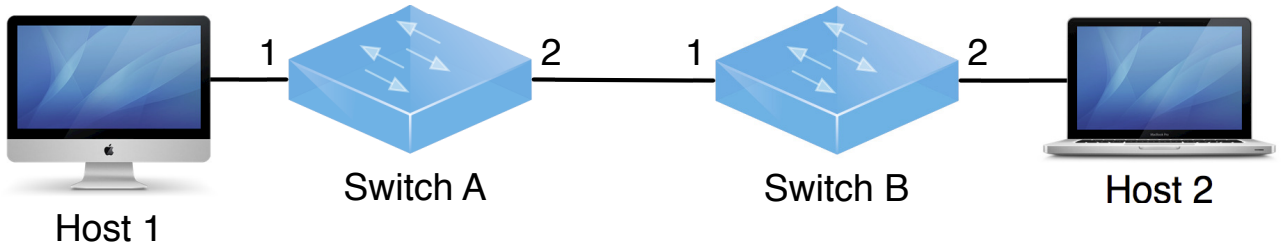
Another example



Forwarding: transfer packets between hosts, *but*
Access control: block SSH packets

Encoding

Forwarding

$$p \triangleq (\mathsf{dst} = H_1 \cdot \mathsf{pt} \leftarrow 1) + (\mathsf{dst} = H_2 \cdot \mathsf{pt} \leftarrow 2)$$

Access Control

$$p_{AC} \triangleq \neg(\mathsf{typ} = \mathrm{SSH}) \cdot p$$

$$p_A \triangleq (\mathsf{sw} = A \cdot \neg(\mathsf{typ} = \mathrm{SSH}) \cdot p) + (\mathsf{sw} = B \cdot p)$$

$$p_B \triangleq (\mathsf{sw} = A \cdot p) + (\mathsf{sw} = B \cdot \neg(\mathsf{typ} = \mathrm{SSH}) \cdot p)$$

Properties

Are non-SSH packets forwarded?
Are SSH packets dropped?
Are p_AC, p_A, and p_B equivalent?

Correct forwarding

$$\left(\begin{array}{l}\mathsf{typ} = \mathrm{SSH} \cdot \mathsf{sw} = A \cdot \mathsf{pt} = 1 \cdot \\ (p_{AC} \cdot t)^* \cdot \\ \mathsf{sw} = B \cdot \mathsf{pt} = 2\end{array}\right) \equiv 0$$

$$\begin{array}{l}\quad (\neg(\mathsf{typ} = \mathrm{SSH}) \cdot \mathsf{sw} = A \cdot \mathsf{pt} = 1 \cdot \mathsf{sw} \leftarrow B \cdot \mathsf{pt} \leftarrow 2) \\ \leq (p_{AC} \cdot t)^*\end{array}$$

Equivalence

$$in \cdot \text{SSH} \cdot (p_A \cdot t)^* \cdot out \equiv in \cdot \text{SSH} \cdot (p_B \cdot t)^* \cdot out$$

Proof

$$
\begin{aligned}
& in \cdot \text{SSH} \cdot (p_A \cdot t)^* \cdot out \\
\equiv & \{ \text{KAT-INVARIANT, definition } p_A \} \\
& in \cdot \text{SSH} \cdot ((a_A \cdot \neg\text{SSH} \cdot p + a_B \cdot p) \cdot t \cdot \text{SSH})^* \cdot out \\
\equiv & \{ \text{KA-SEQ-DIST-R} \} \\
& in \cdot \text{SSH} \cdot (a_A \cdot \neg\text{SSH} \cdot p \cdot t \cdot \text{SSH} + a_B \cdot p \cdot t \cdot \text{SSH})^* \cdot out \\
\equiv & \{ \text{KAT-COMMUTE} \} \\
& in \cdot \text{SSH} \cdot (a_A \cdot \neg\text{SSH} \cdot \text{SSH} \cdot p \cdot t + a_B \cdot p \cdot t \cdot \text{SSH})^* \cdot out \\
\equiv & \{ \text{BA-CONTRA} \} \\
& in \cdot \text{SSH} \cdot (a_A \cdot 0 \cdot p \cdot t + a_B \cdot p \cdot t \cdot \text{SSH})^* \cdot out \\
\equiv & \{ \text{KA-SEQ-ZERO/ZERO-SEQ, KA-PLUS-COMM, KA-PLUS-ZERO} \} \\
& in \cdot \text{SSH} \cdot (a_B \cdot p \cdot t \cdot \text{SSH})^* \cdot out
\end{aligned}
$$

$$
\begin{aligned}
& in \cdot \text{SSH} \cdot (a_B \cdot p \cdot t \cdot \text{SSH})^* \cdot out \\
\equiv & \{ \text{ KA-Unroll-L } \} \\
& in \cdot \text{SSH} \cdot (1 + (a_B \cdot p \cdot t \cdot \text{SSH}) \cdot (a_B \cdot p \cdot t \cdot \text{SSH})^*) \cdot out \\
\equiv & \{ \text{ KA-Seq-Dist-L, KA-Seq-Dist-R, definition } out \} \\
& in \cdot \text{SSH} \cdot a_B \cdot a_2 + \\
& in \cdot \text{SSH} \cdot a_B \cdot p \cdot t \cdot \text{SSH} \cdot (a_B \cdot p \cdot t \cdot \text{SSH})^* \cdot a_B \cdot a_2 \\
\equiv & \{ \text{ KAT-Commute } \} \\
& in \cdot a_B \cdot \text{SSH} \cdot a_2 + \\
& in \cdot a_B \cdot \text{SSH} \cdot p \cdot t \cdot \text{SSH} \cdot (a_B \cdot p \cdot t \cdot \text{SSH})^* \cdot a_B \cdot a_2 \\
\equiv & \{ \text{ Lemma 1 } \} \\
& 0 + 0 \\
\equiv & \{ \text{ KA-Plus-Idem } \} \\
& 0 \\
\equiv & \{ \text{ KA-Plus-Idem } \} \\
& 0 + 0
\end{aligned}
$$

...

$$
\begin{aligned}
\equiv & \{ \text{ KAT-Invariant, definition } p_B \} \\
& in \cdot \text{SSH} \cdot (p_B \cdot t)^* \cdot out
\end{aligned}
$$