CS144
An Introduction to Computer Networks

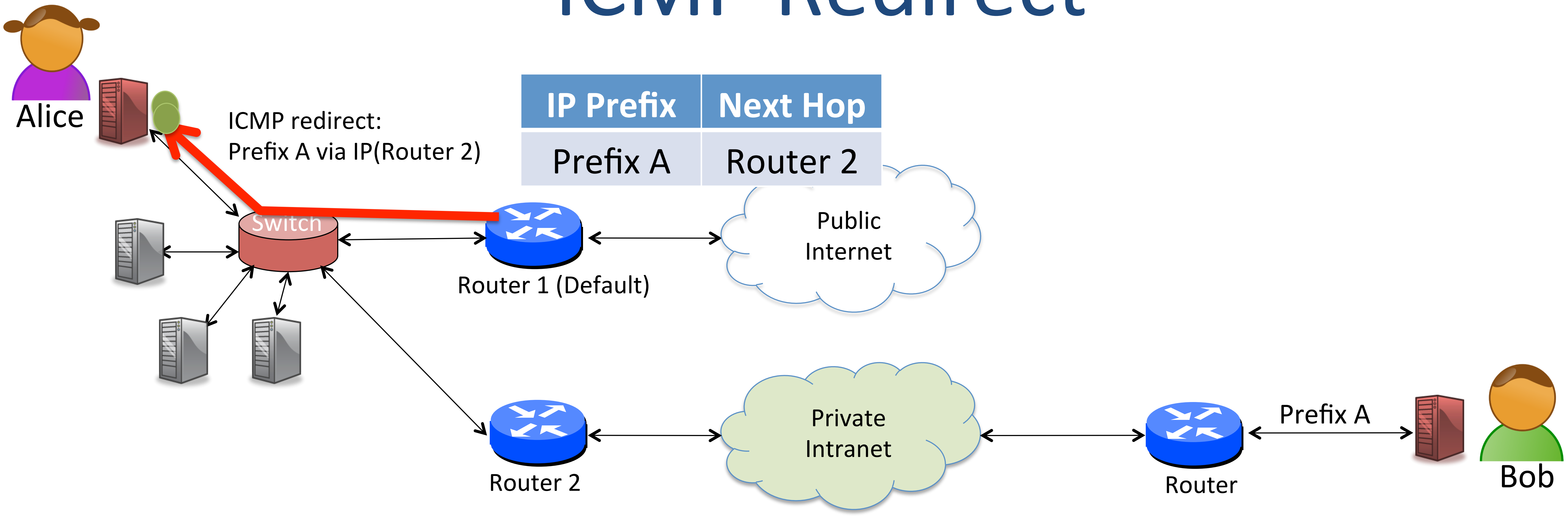
Layer 3 Attacks

Nick McKeown
Professor of Electrical Engineering
and Computer Science, Stanford University

Common types of attack at Layer 3

1. **Use ICMP to tell source end-host to redirect traffic.**
   - Send ICMP redirect messages to source host.
2. **BGP hijacking.**
   - ISP advertises prefix belonging to someone else; capturing their traffic.
   - ISP advertises invalid ISP path, creating “black hole” for traffic.
   - Requires masquerading as ISP, or taking over BGP TCP session.
3. **More specific prefix**.
   - Insert more specific prefix to divert a portion of an address space.
   - Requires masquerading as ISP, or taking over BGP TCP session.

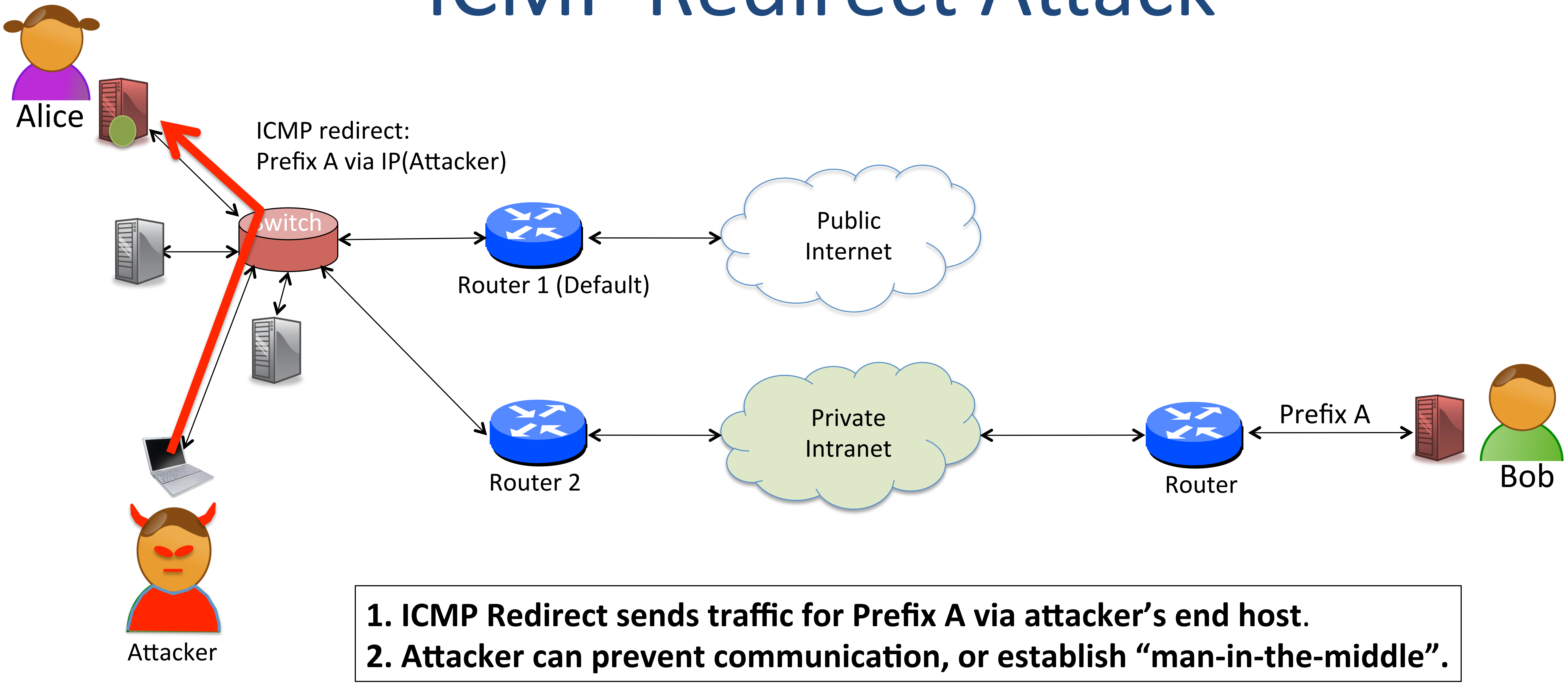
ICMP Redirect



IP Prefix	Next Hop
Prefix A	Router 2

ICMP redirect:
Prefix A via IP(Router 2)

ICMP Redirect Attack



1. **ICMP Redirect sends traffic for Prefix A via attacker's end host.**
2. **Attacker can prevent communication, or establish "man-in-the-middle".**

BGP Attacks

Security vulnerabilities in BGP

1. An AS can advertise IP addresses it doesn't own.
2. An AS cannot verify that an ASpath is correct.
3. ISPs exchange BGP messages over a regular TCP session.

Almost any ISP can bring down the Internet.

(accidentally or maliciously)

Some Examples

2008: Pakistan Telecom

- tried to block access to YouTube
- inadvertently propagated false BGP advertisements

2004: DataOne in Malaysia

- Hijacked two of Yahoo’s Santa Clara prefixes
- Believed by many to be malicious (to block Yahoo)

2003: Spammers hijack Northrop Grumman

- Hijacked block of unused IP addresses
- Used to send spam

Some Examples

2004: Turkish ISP - TTNet

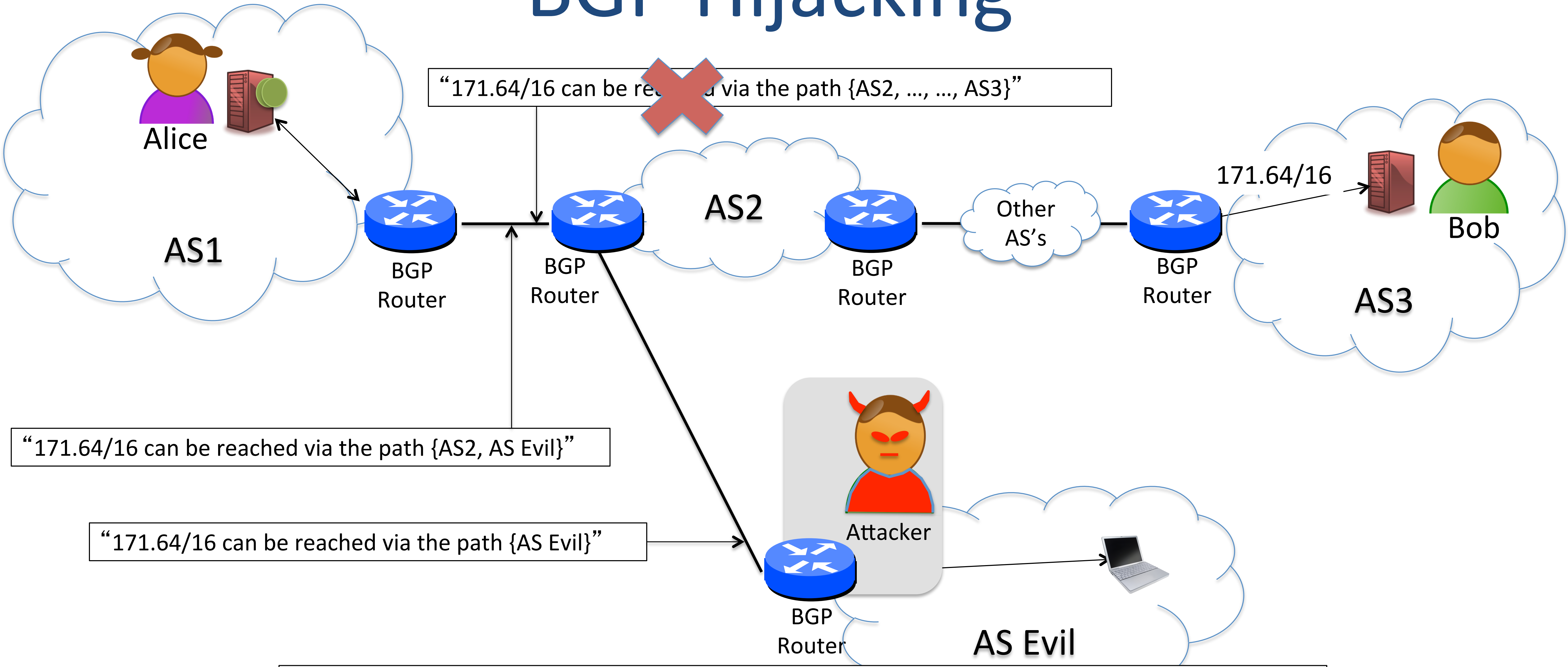
- TTNet sent full BGP routing table; best path via Turkey to everywhere
- Almost entire Internet routed via Turkey
- Most of Internet inoperational for several hours

2008: Brazil

- CTBC sent full BGP routing table that almost hijacked other carriers.
- Luckily, a BGP monitor noticed in time.
- Believed by many to be malicious (to block Yahoo).

[…] Many more!

BGP Hijacking



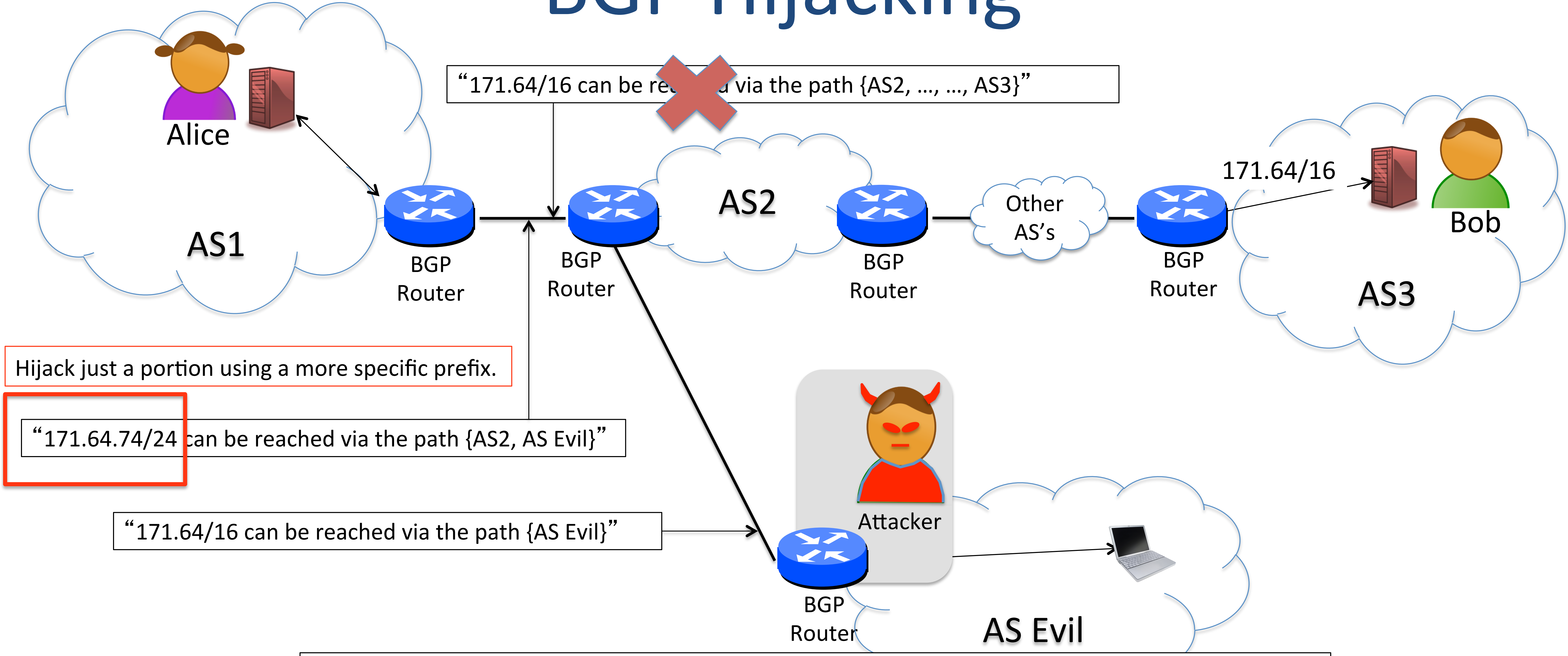
“171.64/16 can be re d via the path {AS2, …, …, AS3}”

“171.64/16 can be reached via the path {AS2, AS Evil}”

“171.64/16 can be reached via the path {AS Evil}”

1. BGP AS_Path advertisement redirects Bob’s traffic to Attacker.
2. Attacker can prevent communication, or establish “man-in-the-middle”.

BGP Hijacking



“171.64/16 can be re d via the path {AS2, …, …, AS3}”

Hijack just a portion using a more specific prefix.

“171.64.74/24 can be reached via the path {AS2, AS Evil}”

“171.64/16 can be reached via the path {AS Evil}”

1. BGP AS_Path advertisement redirects Bob’s traffic to Attacker.
2. Attacker can prevent communication, or establish “man-in-the-middle”.

<The End>