

Detecting Large Scale Eavesdropping


Ashok Chokalingam

Disclaimer

The following information should not be used for malicious purposes or intent

The information contained in this Presentation is for educational purposes ONLY!

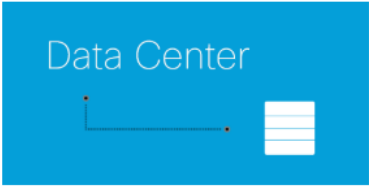
Routers Uptime


 Cisco Blogs

Log In to Cisco.com

All BlogsTechnologiesIndustriesPartnersFor the Tech ExpertGet to Know CiscoCountries and Regions

Cisco Blog > Data Center



Data Center
What is the longest running item of Cisco equipment in your data center? Can you beat 13 years?

Stephen Speirs
June 18, 2012 ~ 2 Comments

Where were you in 1998? Somewhere in one of our customers, a customer booted one of our 3640 routers, and it's been running ever since without a reboot!







It's been running since last century! Wow. It's been running since around the time my daughter was born, and a good few years before my son was born! It's been running longer than some of our competitors have been in existence, and longer than [Juniper Networks](#) has been a publicly traded company!

I learned this from an email that was passed around my office, that highlighted this remarkable evidence of reliability. It made me wonder, in your data center, what is your longest running piece of Cisco data center equipment?

And it also reminded me of some of our best practices for network reliability, such as Cisco Smart Services, described in this short VoD:

Subscribe to Data Center:

Subscribe

Connect with Data Center


Cisco Social Rewards
The current version of the Social Rewards program will be discontinued in August 2018.
Cisco Blogs is looking for better ways to engage our entire Cisco community across all Cisco properties.
[Read More](#)

Router Uptime

show ver

Cisco Internetwork Operating System Software IOS (tm) 3000 Software (IGS-J-L), Version 11.1(8), RELEASE SOFTWARE (fc1) Copyright (c) 1986-1996 by cisco Systems, Inc. Compiled Thu 05-Dec-96 11:41 by tamb Image text-base: 0x03038820, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE ROM: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)

uptime is 17 years, 14 weeks, 5 days, 16 hours, 47 minutes

System restarted by reload at 10:39:13 CST Wed Jan 29 1997 System image file is "flash:igs-j-l_111-8.bin", booted via flash Network configuration file is "#####", booted via tftp from #####

cisco 2500 (68030) processor (revision D) with 16384K/2048K bytes of memory. Processor board ID 03217044, with hardware revision 00000000 Bridging software. SuperLAT software copyright 1990 by Meridian Technology Corp). X.25 software, Version 2.0, NET2, BFE and GOSIP compliant. TN3270 Emulation software (copyright 1994 by TGV Inc). 2 Ethernet/IEEE 802.3 interfaces. 2 Serial network interfaces. 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

[permalink](#) [embed](#) [save](#)

[load more comments](#) (4 replies)

[-] [notsoevilbryan](#) [CCNP](#) 12 points 4 years ago

At my new gig I found an old 3550 in our datacenter running ilo. Don't have the heart to replace it yet.

uptime is 10 years, 32 weeks, 1 hour, 41 minutes System returned to ROM by power-on

System restarted at 16:42:37 EST Mon Sep 29 2003.

[permalink](#) [embed](#) [save](#)

In This Presentation We'll Cover

- How large scale Eavesdropping works!
- How an routing protocol like OSPF is used for traffic redirection
 1. Refresher Routing/ospf
 2. Adversary joining OSPF Neighborhood as rouge
 3. Adversary Breaking OSPF Authentication
 4. DNS poisoning/Eavesdropping/traffic Redirection
 5. Manipulating the OSPF database with a single packet to blackhole an Entire segment
- How to monitor Large Scale Eavesdropping

Routers/Routing Refresher

- Adding routes manually is called static routing
- Gateway is the next hop router to get there. Even if the subnet is multiple routers away, we only specify the next hop router.



Autonomous System

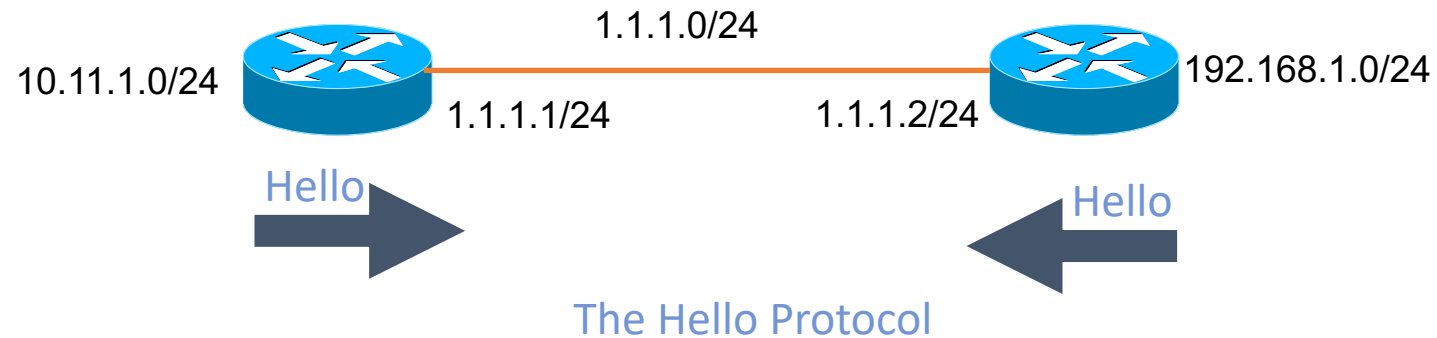
IGP (interior Gateway Protocol)

- OSPF
- RIP
- EIGRP
- IS-IS

How OSPF Works(Open Shortest Path First)

Uses Link State Logic

1. Neighbor Discovery
2. Topology Database Exchange
3. Faster Route Computation



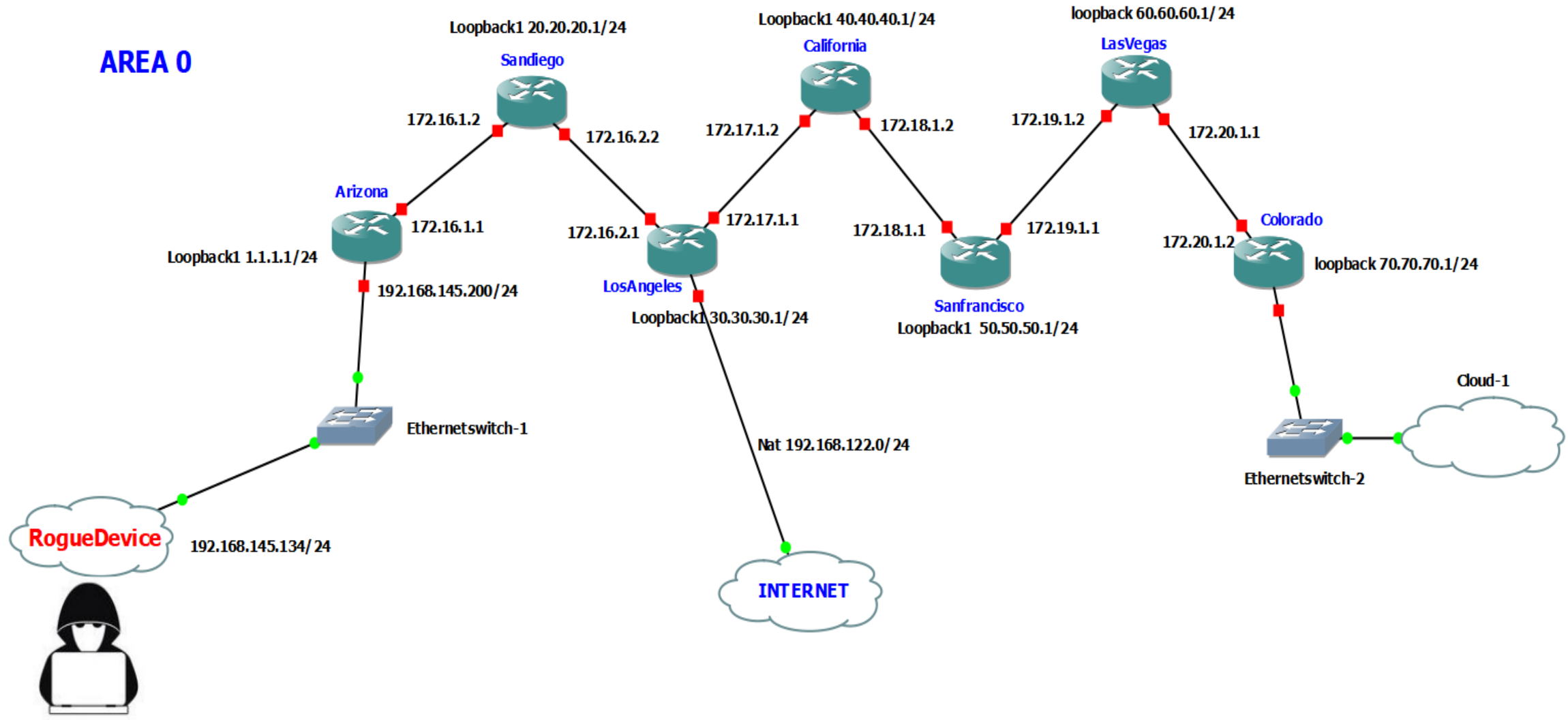
How OSPF Works

- When a link comes up and routers exchange hellos they are in a two-way state.
- Hellos are sent to 224.0.0.5 – All OSPF routers multicast address.
- Once hellos are exchanged, the following parameter checks are made:
 - Must pass authentication
 - Same primary subnet (Cisco)
 - Same OSPF area
 - Same area type
 - Can't have duplicate RIDs
 - Hello and Dead timers must be the same
- Hello interval is 10 seconds on standard ethernet interfaces.
- The dead timer defaults to 4 times the hello interval.

How OSPF Works

- Every router periodically advertises its link state (i.e. “who are my neighbors?”). – This is called Link State Advertisement (LSA).
- The LSAs are flooded throughout the network hop-by-hop.
- Every router receives the LSAs of all other routers
 - and installs it in its LSA DB
 - this allows to build the topology map of the AS.
- There are several types of LSAs. The most important one is:
Router LSA – contains the links of a given router

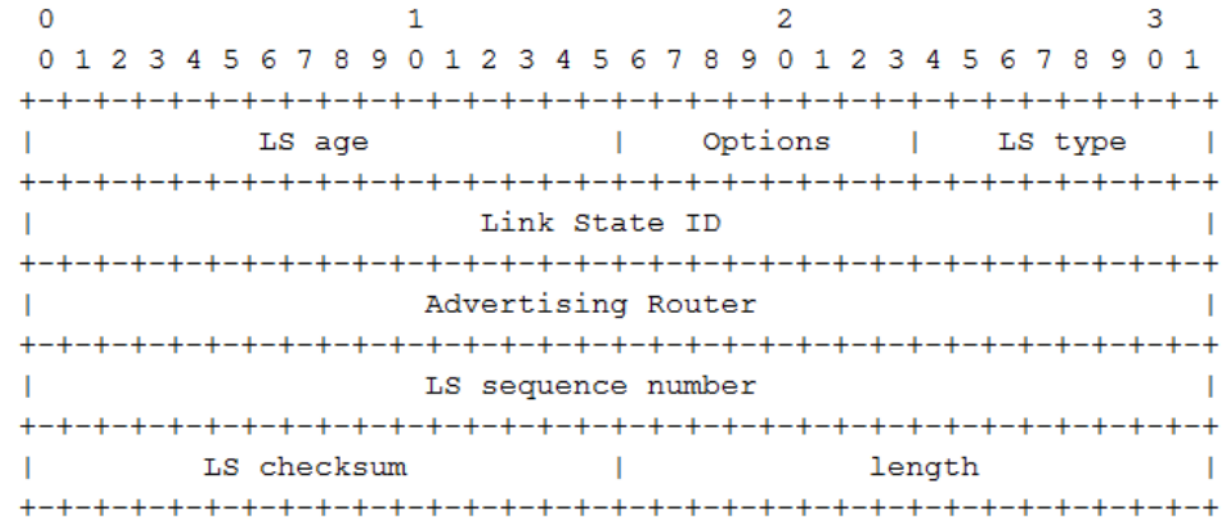
GNS3 Demo Architecture



Owning The Routing Table

- a) The attack is based on analysis of the OSPF specification [RFC 2328] presented in blackhat. Several Advisories had been released by vendors.
- b) one can control the entire routing domain with a single packet.
- c) Only a single well-crafted attack packet is required

Link state Advertisement Header



An LSA is uniquely identified by:

- LS type (for Router LSA it is always '1')
- Advertising Router
- Link State ID

Advertising Router ID VS Linkstate ID

- Advertising Router – identifies the router that originated the LSA.
 - i.e., the router ID
- Link State ID – identifies the part of the AS that is being described by the LSA.
 - i.e., the router ID

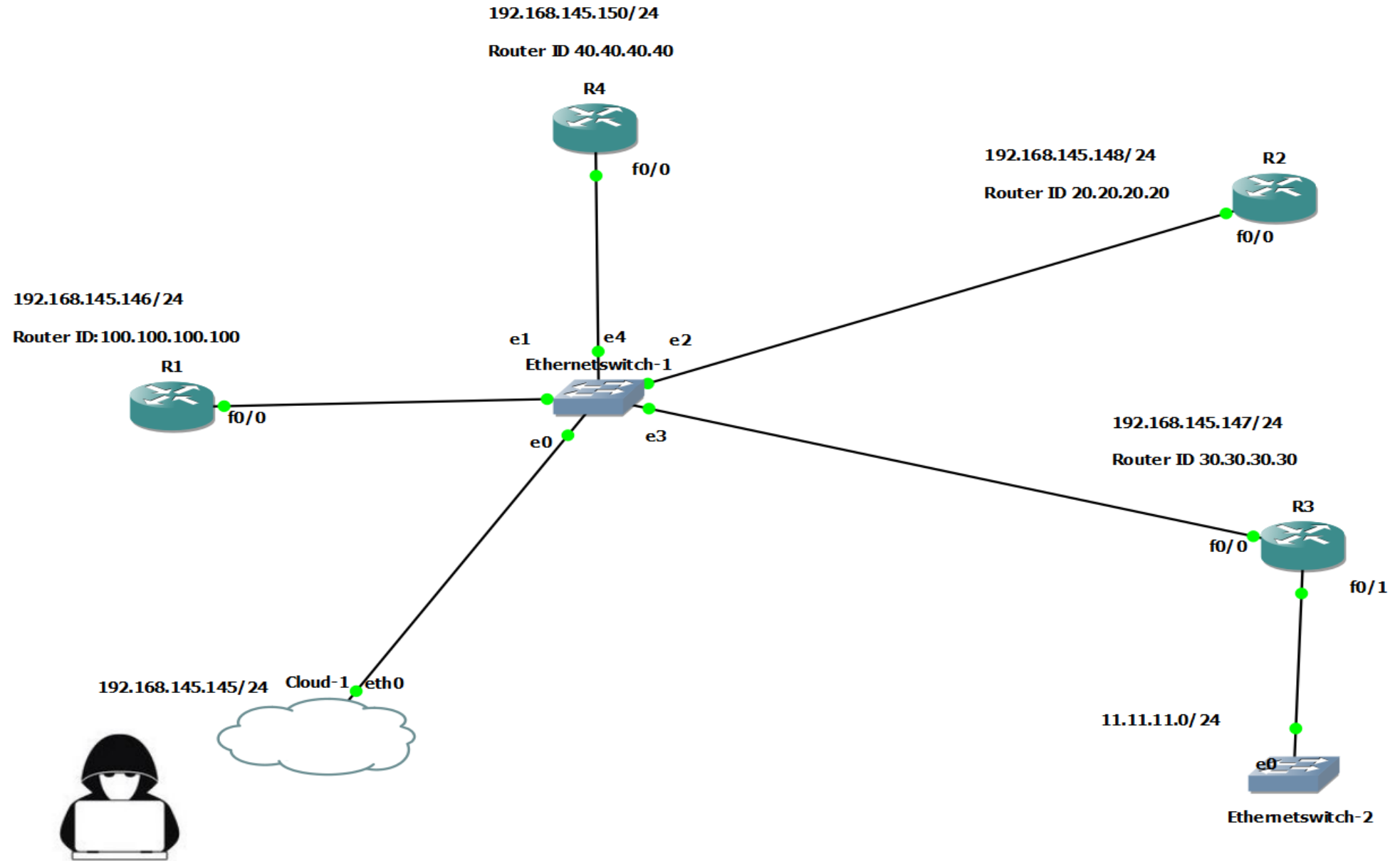
The two fields must have the same value

But, the OSPF spec does not specify a check to verify this on LSA reception!

The Vulnerability Full Poisoning

- According to the OSPF spec (Sec. 13.4)
 - A router fights back only if it receives a false LSA in which
 - “the **Advertising Router** is equal to the router's own Router ID ”
- If the victim router receives a false LSA having:
 - Link State ID = victim router's ID
 - Advertising Router \neq victim router's ID
- Then, no fight back is triggered by the victim!
 - This is despite the fact that the LSA claims to describe links of the victim router itself.

GNS3 single packet Demo



Single packet Revert

If it wishes, the attacker can undo the erasure by sending another false LSA but with an Advertising Router = victim's ID.

References

- <https://media.blackhat.com/us-13/US-13-Nakibly-Ownning-the-Routing-Table-Part-II-WP.pdf>