
BERNE CAMPBELL'S
GHOST RECON
SUBVERTING LOCAL NETWORKS

Why?

- Network Security
- Information Gathering
- Eavesdropping
- MitM
- Invisibility

Objectives

- Recon
  - LLDP
  - OSPF
- MitM
  - VRRP
  - OSPF

Recon

- LLDP
- OSPF

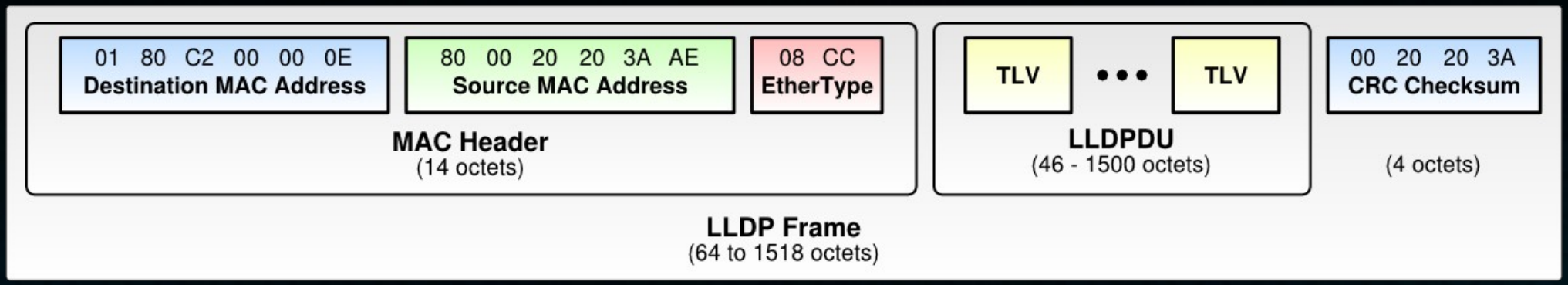
Link Layer Discovery Protocol

- IEEE 802.1AB-2005
- Vendor Neutral
- Similar functionality to CDP, EDP, NDP
- Layer 2
- Multicast MAC 01:80:c2:00:00:0e

LLDP

- TLV based protocol
- Info includes: -
    - System name & desc
    - Port name & desc
    - VLAN
    - IP Management address

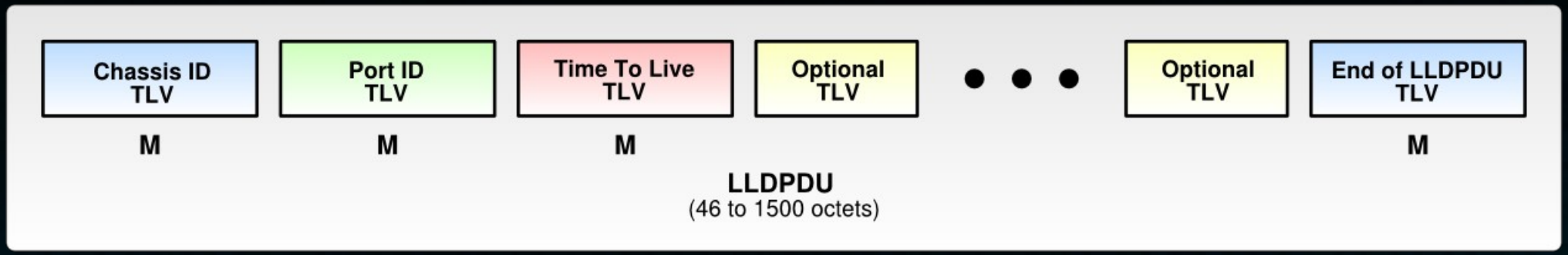
LLDP Frame


01 80 C2 00 00 0E
Destination MAC Address
80 00 20 20 3A AE
Source MAC Address
08 CC
EtherType
MAC Header
(14 octets)
TLV
TLV
LLDPDU
(46 - 1500 octets)
00 20 20 3A
CRC Checksum
(4 octets)
LLDP Frame
(64 to 1518 octets)

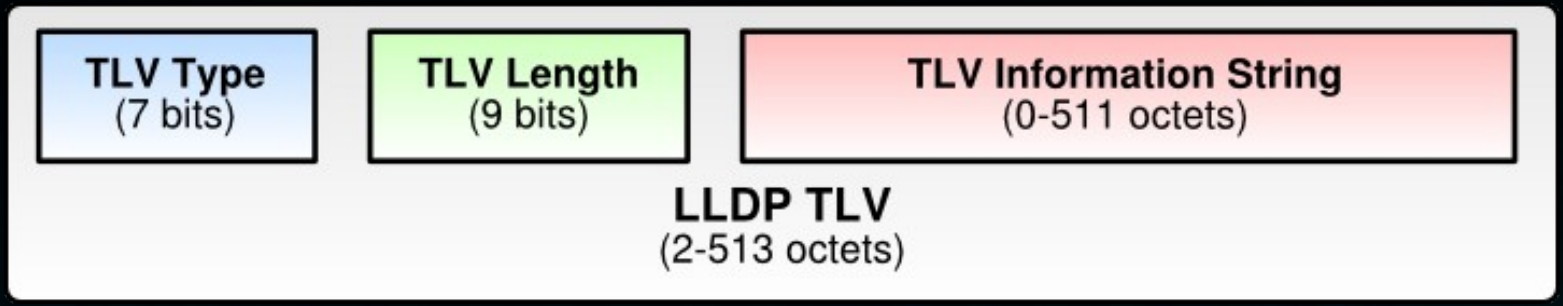
LLDP TLVs

- Mandatory TLVs: -
    - Chassis ID
    - Port ID
    - TTL
    - End of LLDPDU TLV
- Optional TLVs between TTL and EoL

LLDPDU


Chassis ID TLV
Port ID TLV
Time To Live TLV
Optional TLV
Optional TLV
End of LLDPDU TLV
M
M
M
M
LLDPDU
(46 to 1500 octets)

LLDP TLV


TLV Type
(7 bits)
TLV Length
(9 bits)
TLV Information String
(0-511 octets)
LLDP TLV
(2-513 octets)

LLDP Topology Discovery

- SNMP
- Local
    - LLDPD
- Multiple Hops
    - NetDisco
    - Wiremaps

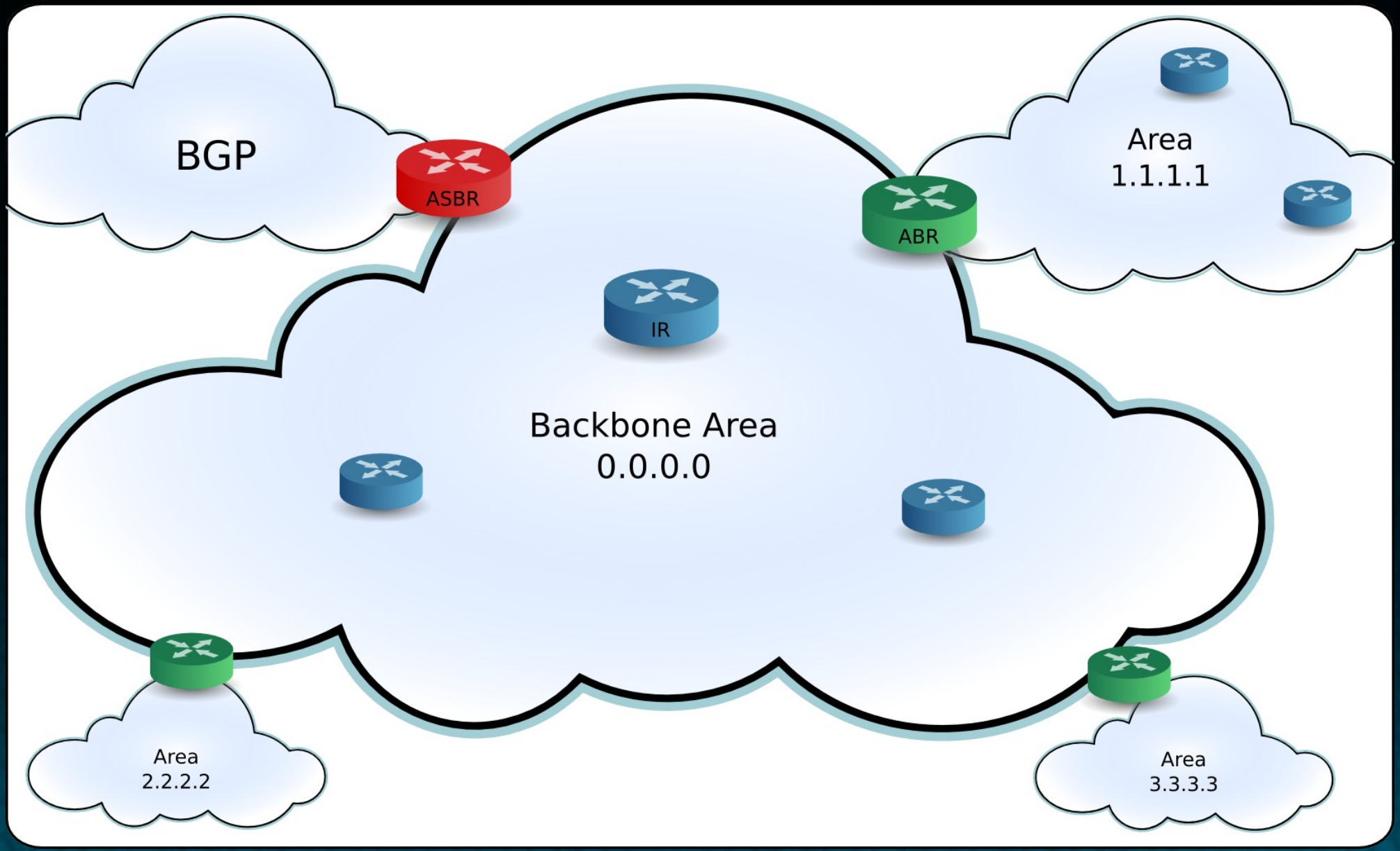
Open Shortest Path First

- Routing Protocol
    - RFC 2328
    - Link State
- Similar to IS-IS
- Simple Authentication
    - Plain-text Password
    - MD5

OSPF Hierarchy

- Areas
  - Backbone == 0.0.0.0
  - Non-backbone != 0.0.0.0
  - All areas connected to backbone
- Routers
  - Internal Routers (IRs)
  - Area Border Routers (ABRs)
  - Autonomous System Border Routers (ASBRs)

OSPF


BGP
ASBR
ABR
Area
1.1.1.1
IR
Backbone Area
0.0.0.0
Area
2.2.2.2
Area
3.3.3.3

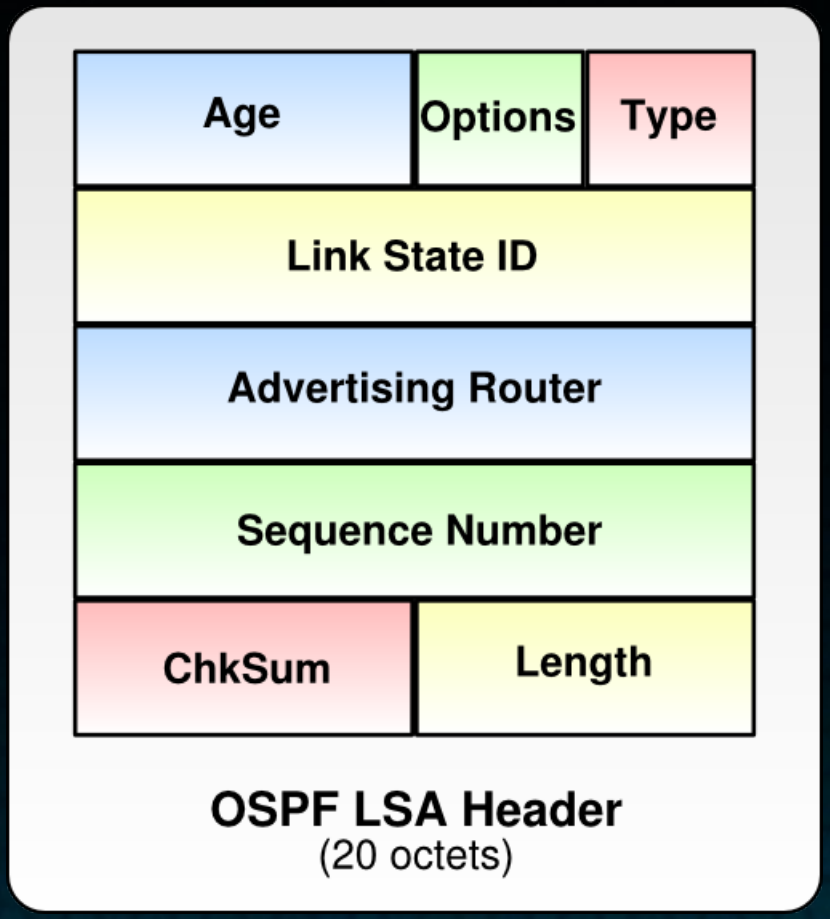
OSPF Link State

- Link State Database
    - Made up of LSAs
- Link State Advertisements (LSAs)
    - Type
    - ID
    - Advertising Router
    - Instance (Seq, Chksum, Age)

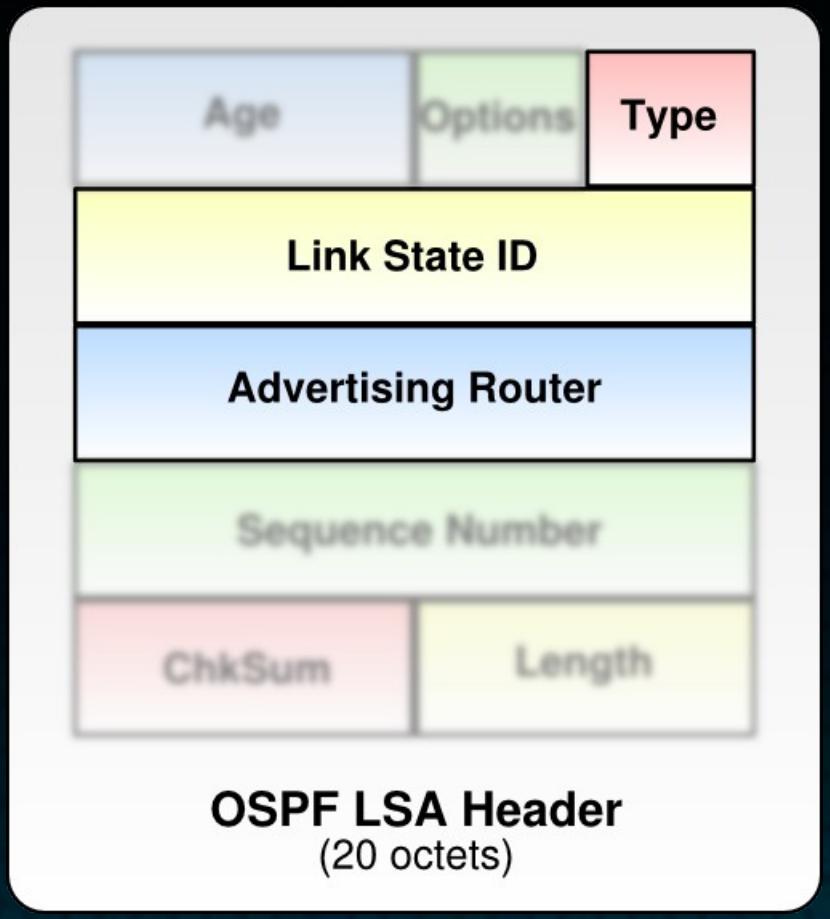
OSPF LSAs

- LSA Types
  - Router LSAs
  - Network LSAs
  - Summary LSAs
  - ASBR Summary LSAs
  - External LSAs

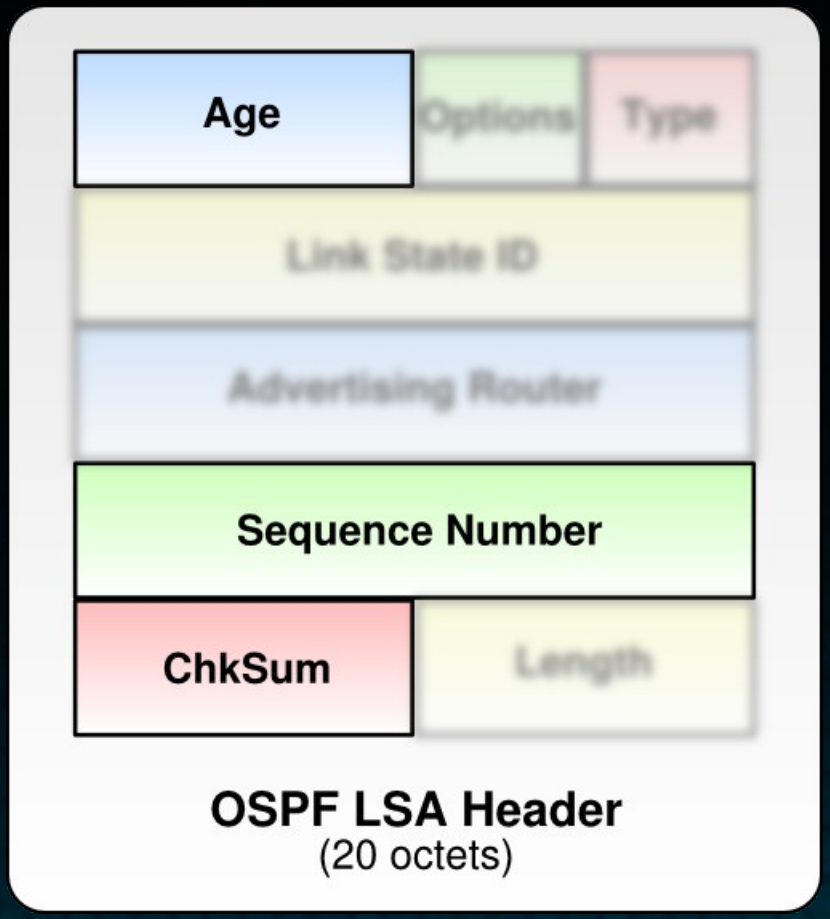
OSPF LSA Header



OSPF LSA Lookup



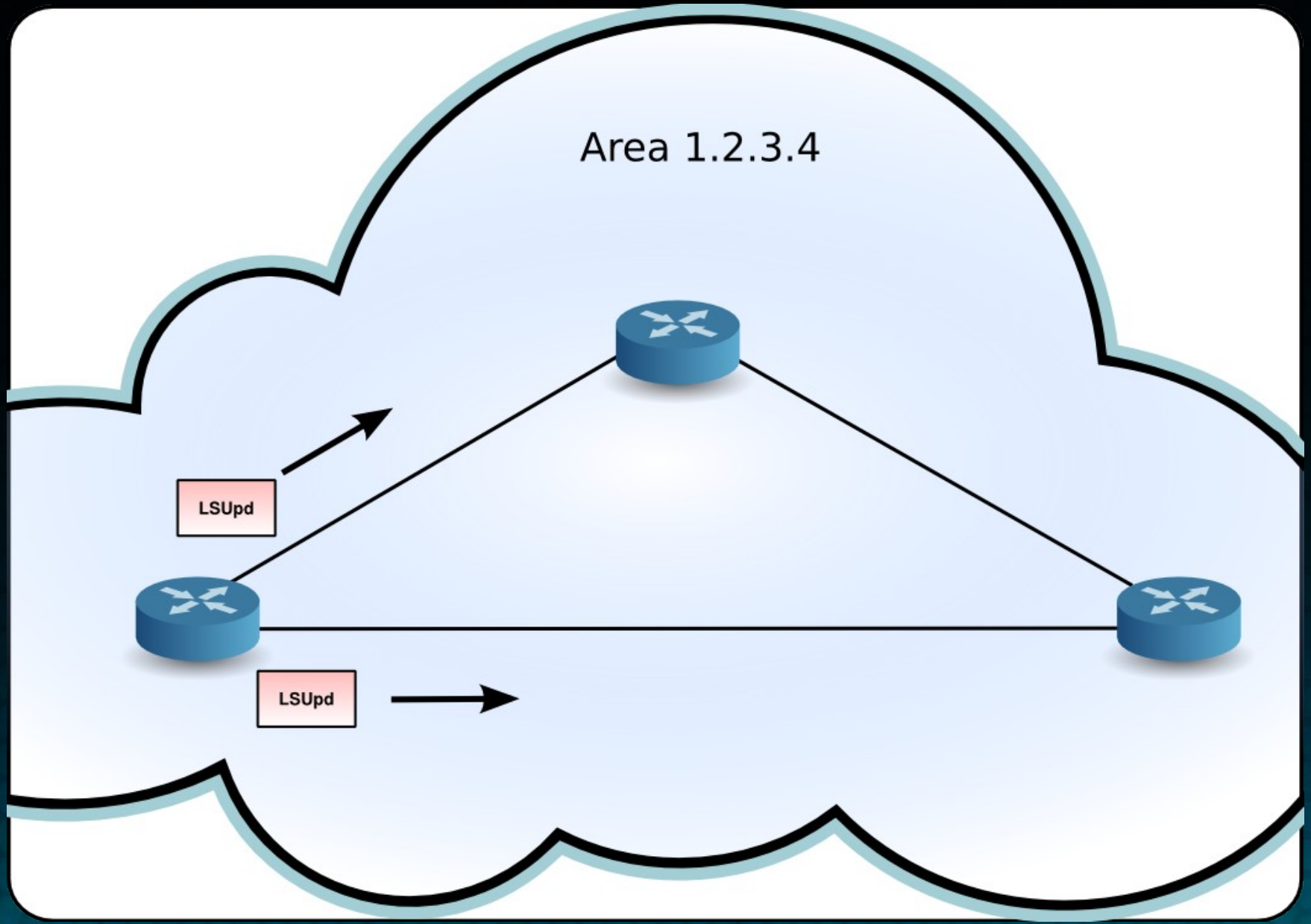
OSPF LSA Instance



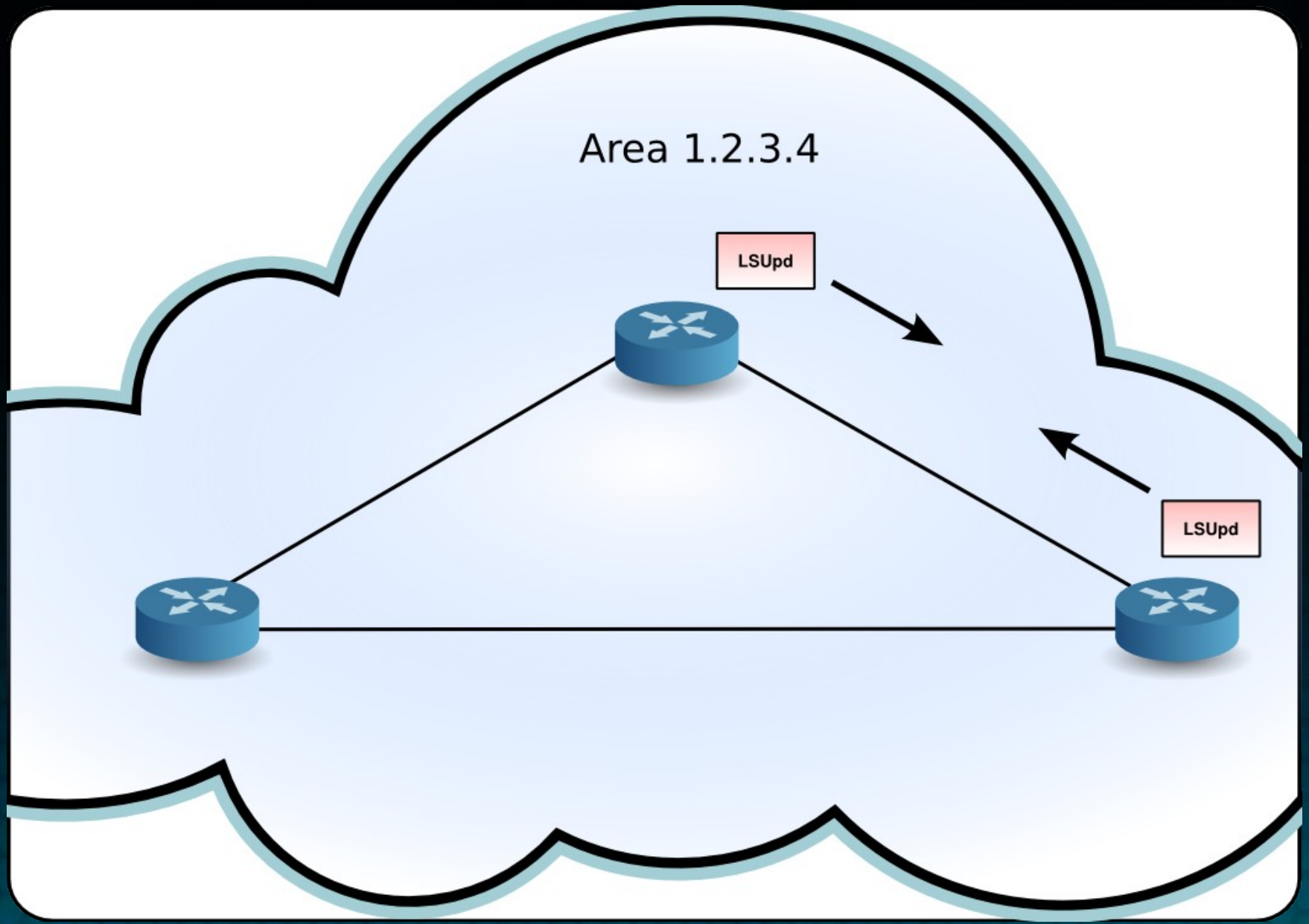
OSPF Neighbourships

- Adjacent Routers form neighbourships
- Exchange link state information
- Flood updates
- Synchronized LS Databases

OSPF Flooding



OSPF Flooding



OSPF Broadcast Networks

- Broadcast networks
  - Multicast 224.0.0.5 and 224.0.0.6
  - Designated Router (DR)
  - Backup Designated Router (BDR)
  - DR originates Network LSA

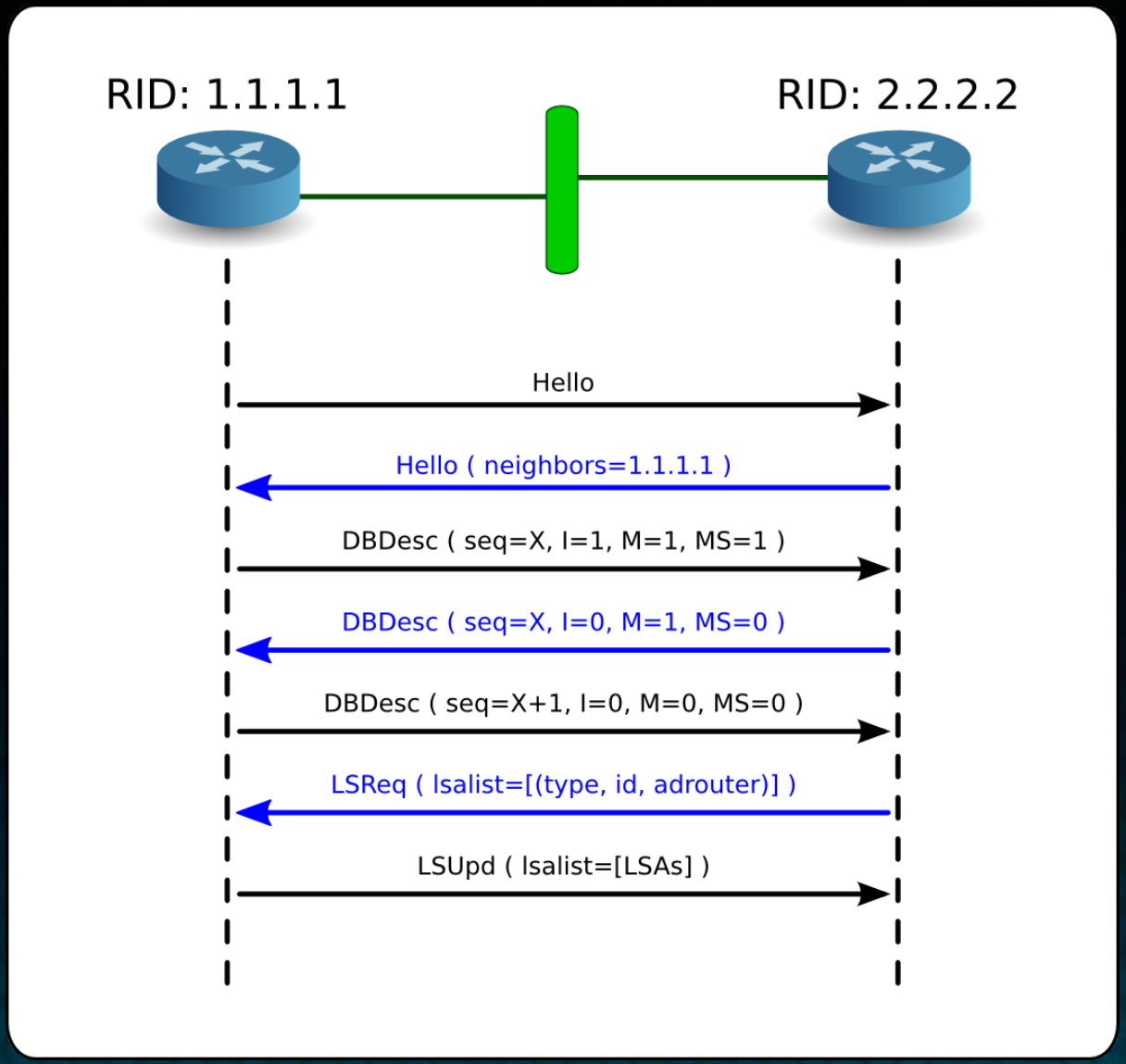
OSPF Topology Discovery

- Passive
    - LSRefreshTime (30 Mins)
- Active
    - Subvert Router
    - Rouge Router
    - Spoof LSA Requests

OSPF Active Topology Discovery

- Router LSAs
    - ID == Advertising Router
- Network LSAs
    - ID == DR's IP
    - Adv Rtr == DR RID
- Limitation with BDR
    - Unknown DR RID

OSPF Forming an Adjacency



ghOSPF

- PoC
- Scapy Add-on
- Discovery of topology
    - Passive
    - Active
- RFC 3514 Compliance

Scapy

- Python Packet Manipulation Tool
- Philippe Biondi
- Decodes rather than interprets
- Replaces numerous tools
- Combine functionality
- Add-ons

Demo

- Recon
  - OSPF

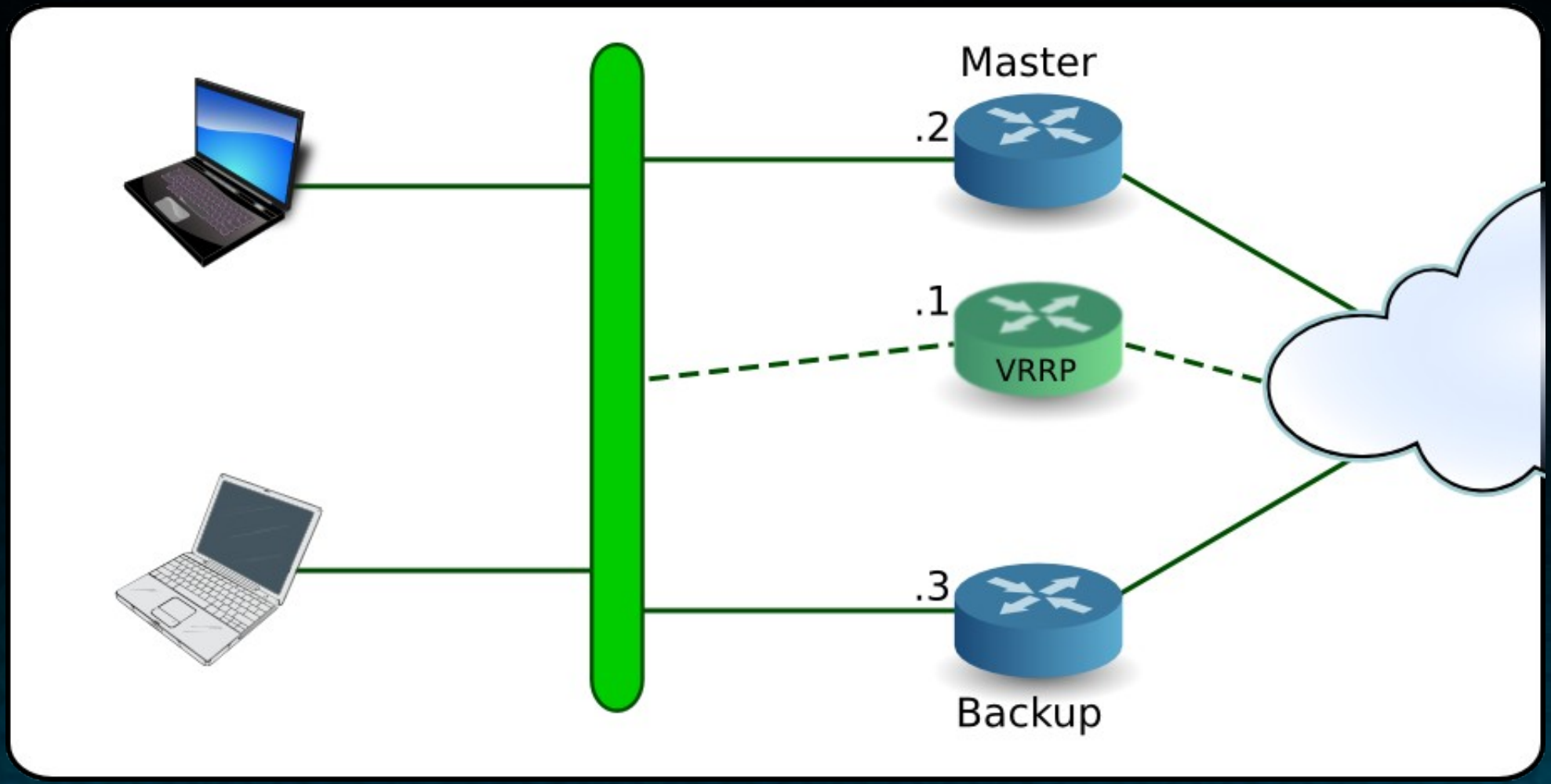
MitM

- VRRP
- OSPF

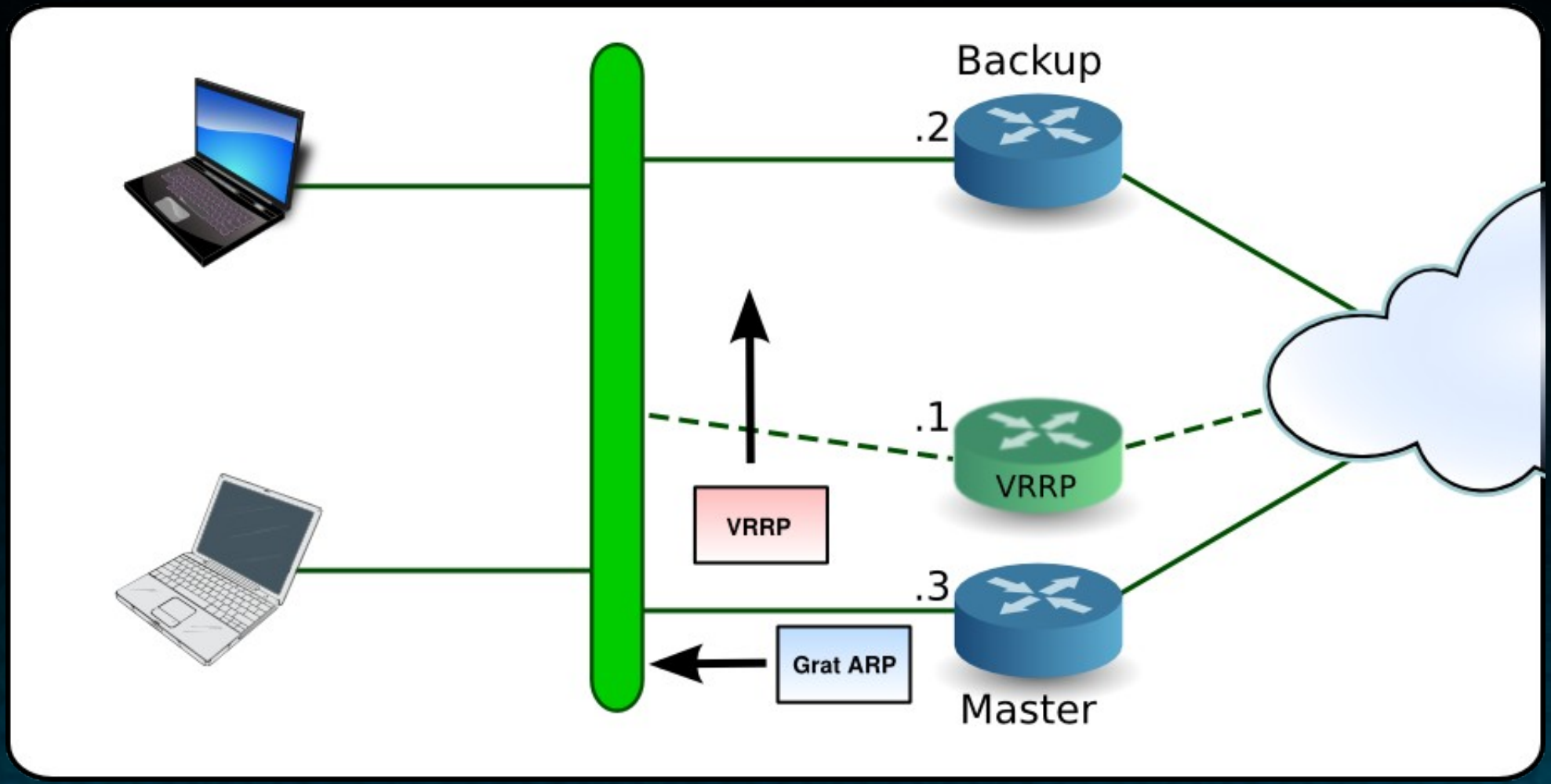
Virtual Router Redundancy Protocol

- First Hop Redundancy
- Provides Fault Tolerance
- Based off Cisco's HSRP
- Layer 3
- Standardized - RFC 3768
- Current version 2
- Uses Gratuitous ARP with BIA MAC

VRRP



VRRP Switchover



VRRP Security

- TTL 255 (directly connected)
- Authentication
  - None
  - Plaintext password
  - MD5 PSK (Non-standard)
  - IPSEC AH
    - Truncated MD5 HMAC
    - Not supported by all implementations

VRRP Pre-empting

- Default Priority 100
- Priority 255 reserved for Owner
- Pre-empting is typical
    - Owner always pre-empts regardless of pre-empt setting
    - Pre-empt on by default

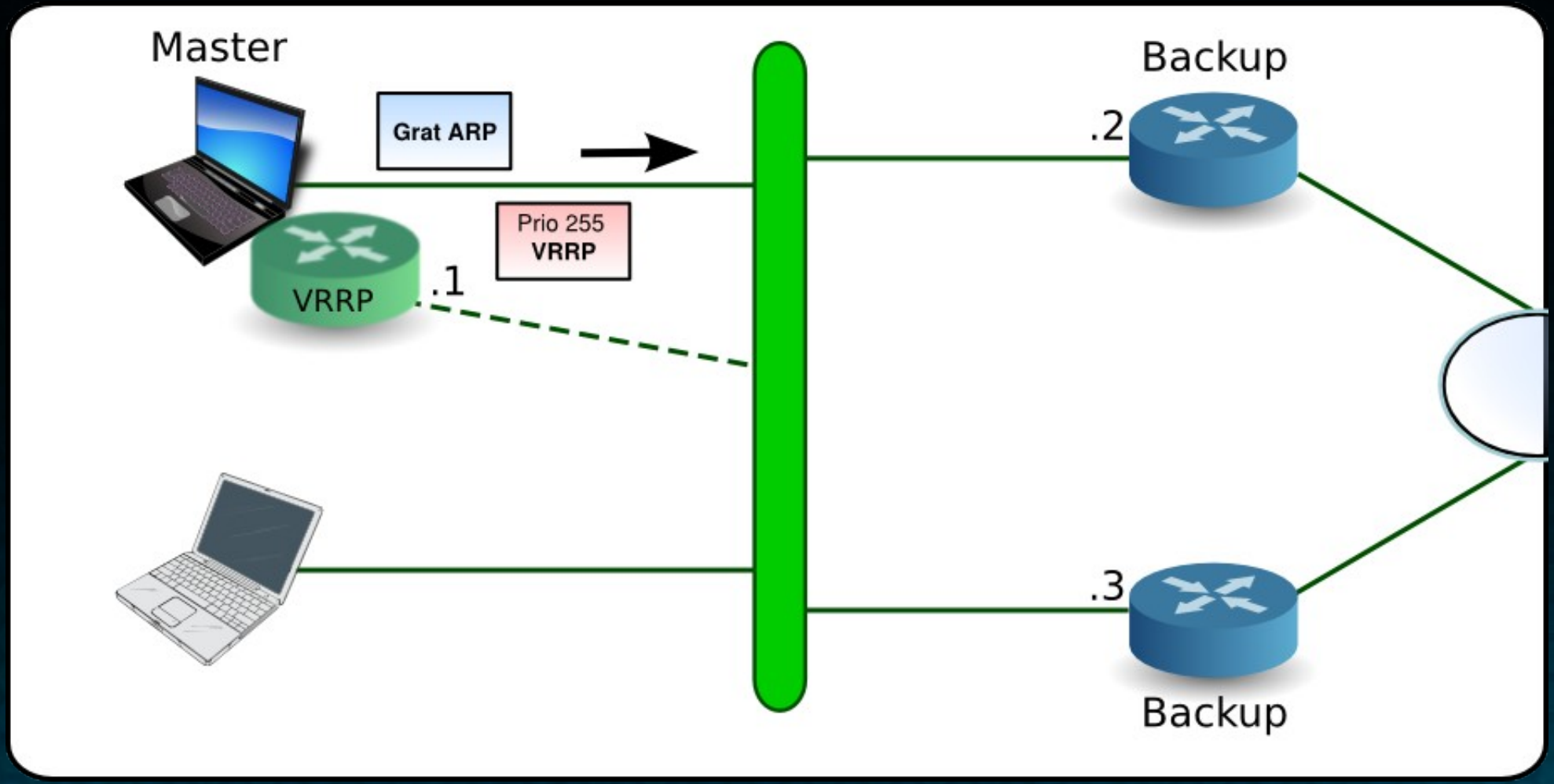
VRRP Switchover

- New-Contestent pips Incumbent Master iff: -
    - NC's Priority > IM's Priority
- Tie-breaker: -
    - NC's Primary IP > IM's Primary IP

VRRP Hostile Takeover

- Local (mcast, TTL 255)
- Send Announcement (Win Election)
    - Priority == 255
    - Tie-breaker: IP > Incumbent's IP
- Send Gratuitous ARPs for virtual IPs
- Periodically send advertisements

VRRP Hostile Takeover



OSPF Attacks

- Compromised Router
- Compromised Network Segment
- OSPF Attack Shell
    - GomoR
- ghOSPF

OSPF Security

- Multicast
- GTSM (optional)
- Authentication
    - Plaintext Password
    - MD5
- Fight Back

ghOSPF

- PoC
- Scapy Add-on
- Discovery of topology
    - Passive
    - Active
- **Route Manipulation/Injection**
- RFC 3514 Compliance

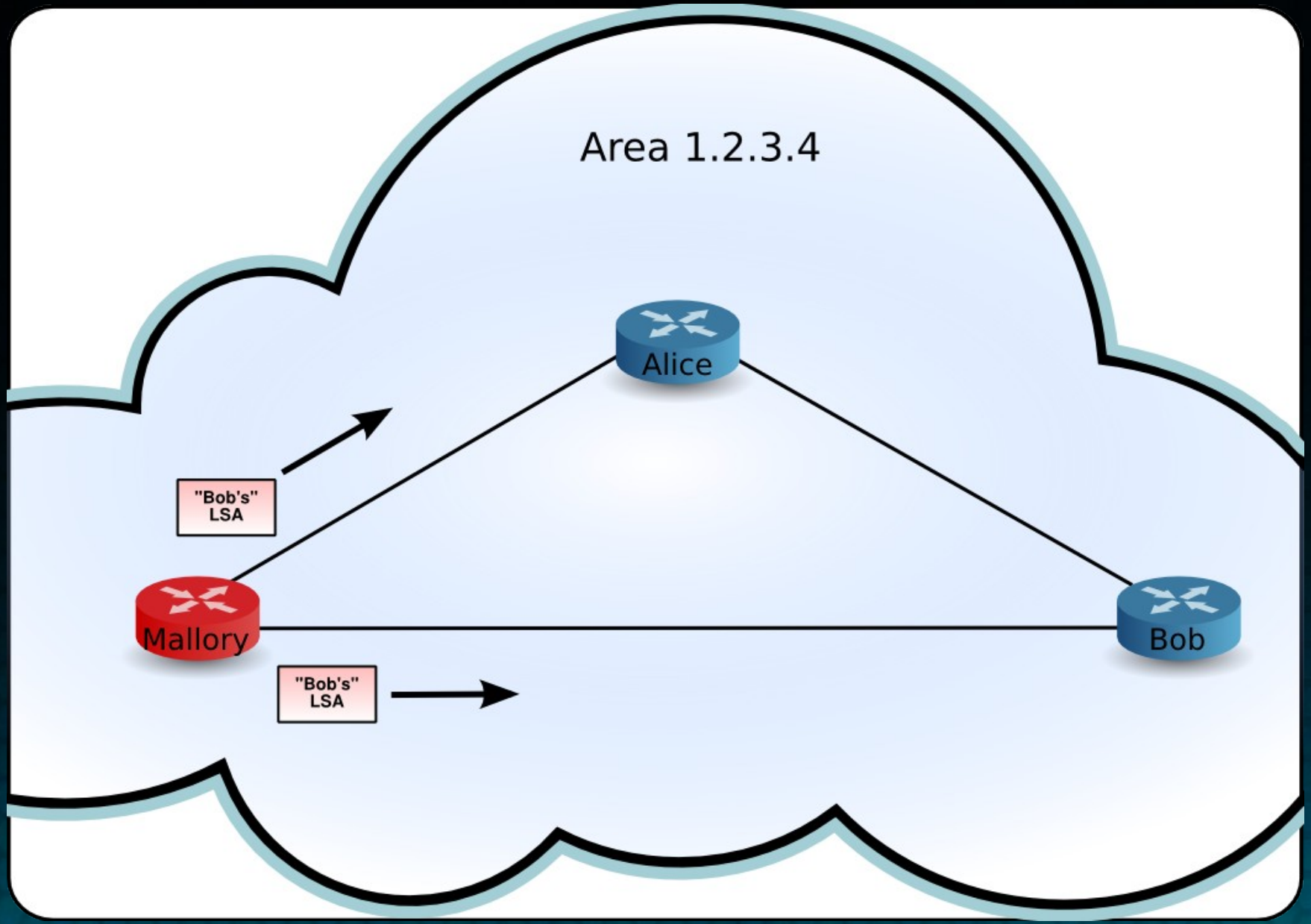
OSPF Route Manipulation

- Routing ← SPF ← LSDB ← LSAs
- Intra > Inter > E1 > E2
- LSA's metrics – cost
- Partitioned LSAs won't go into SPF
- Must spoof LSA(s)
    - Must Fight Fightback

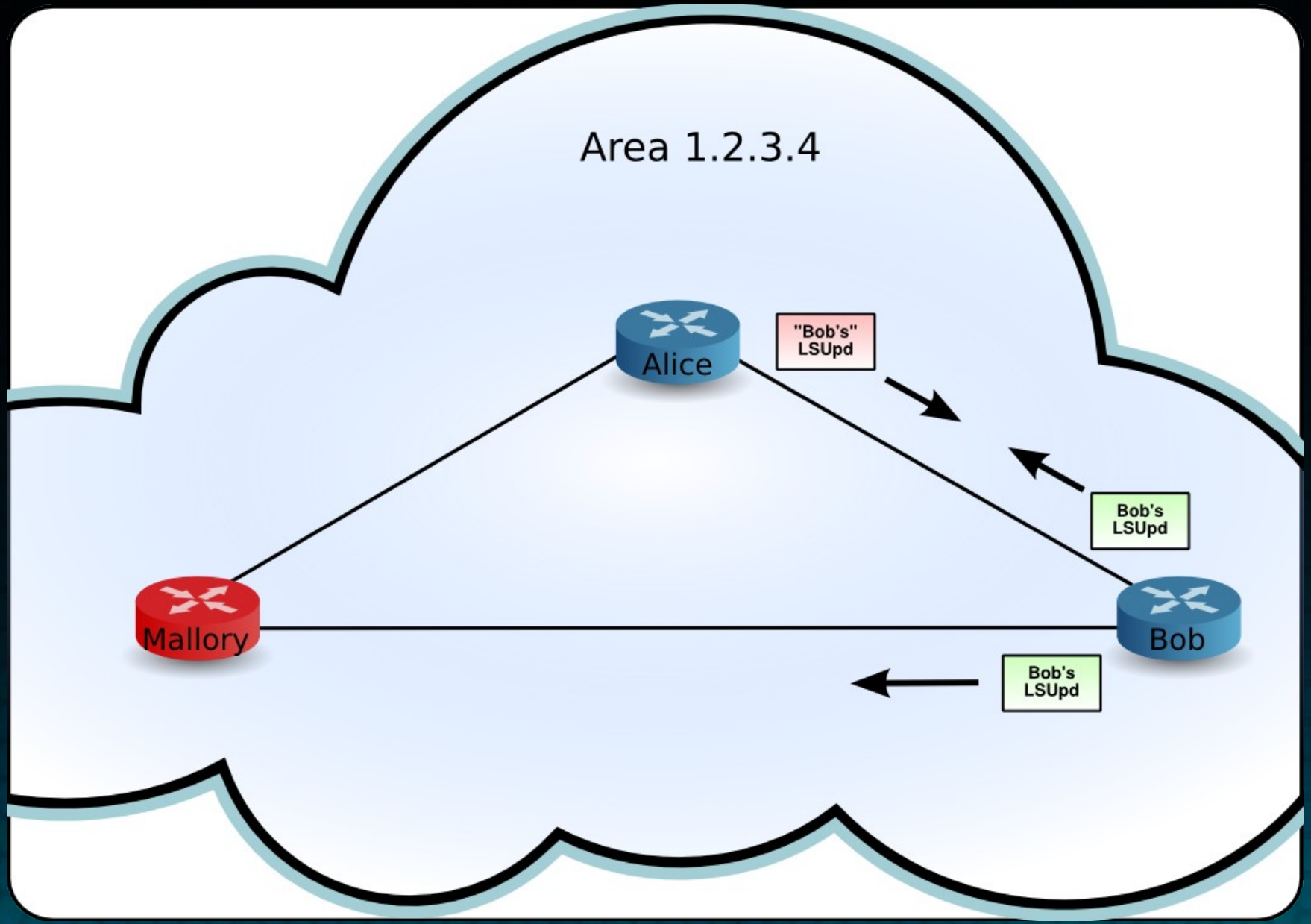
OSPF Fight Back

- Router receives “wrong” LSA
    - Same Advertising Router ID
    - Wrong details though
- Originates new LSA
    - Correct details
    - Newer Seq

OSPF Fight Back



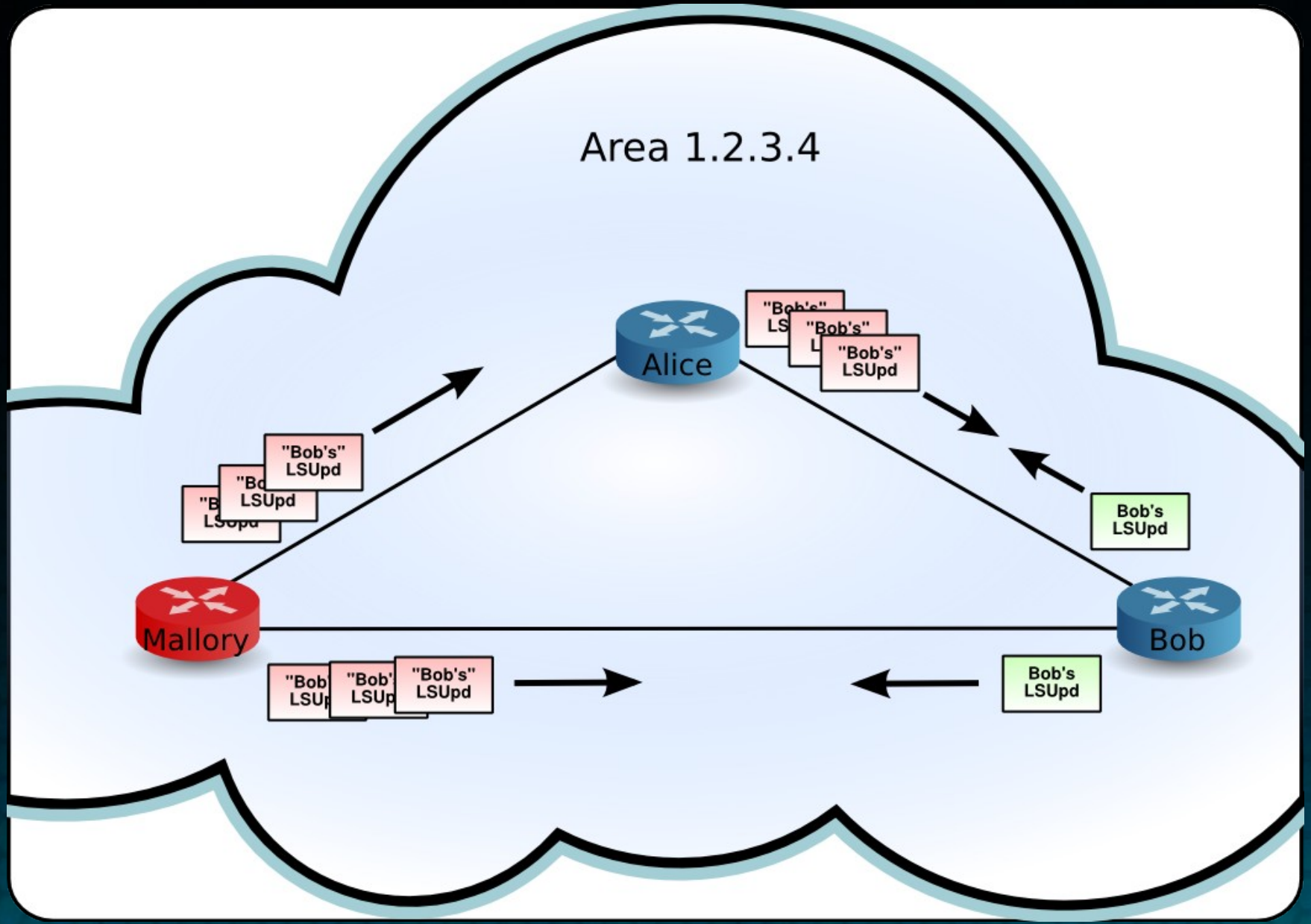
OSPF Fight Back



Defeating OSPF Fight Back

- MinLSInterval
    - 5 seconds
    - Min time before originating LSA
- MinLSArrival
    - 1 second
    - Min time before processing LSA
- Race condition
    - Transmit LSAs @ 1s with > Seq

Defeating OSPF Fight Back

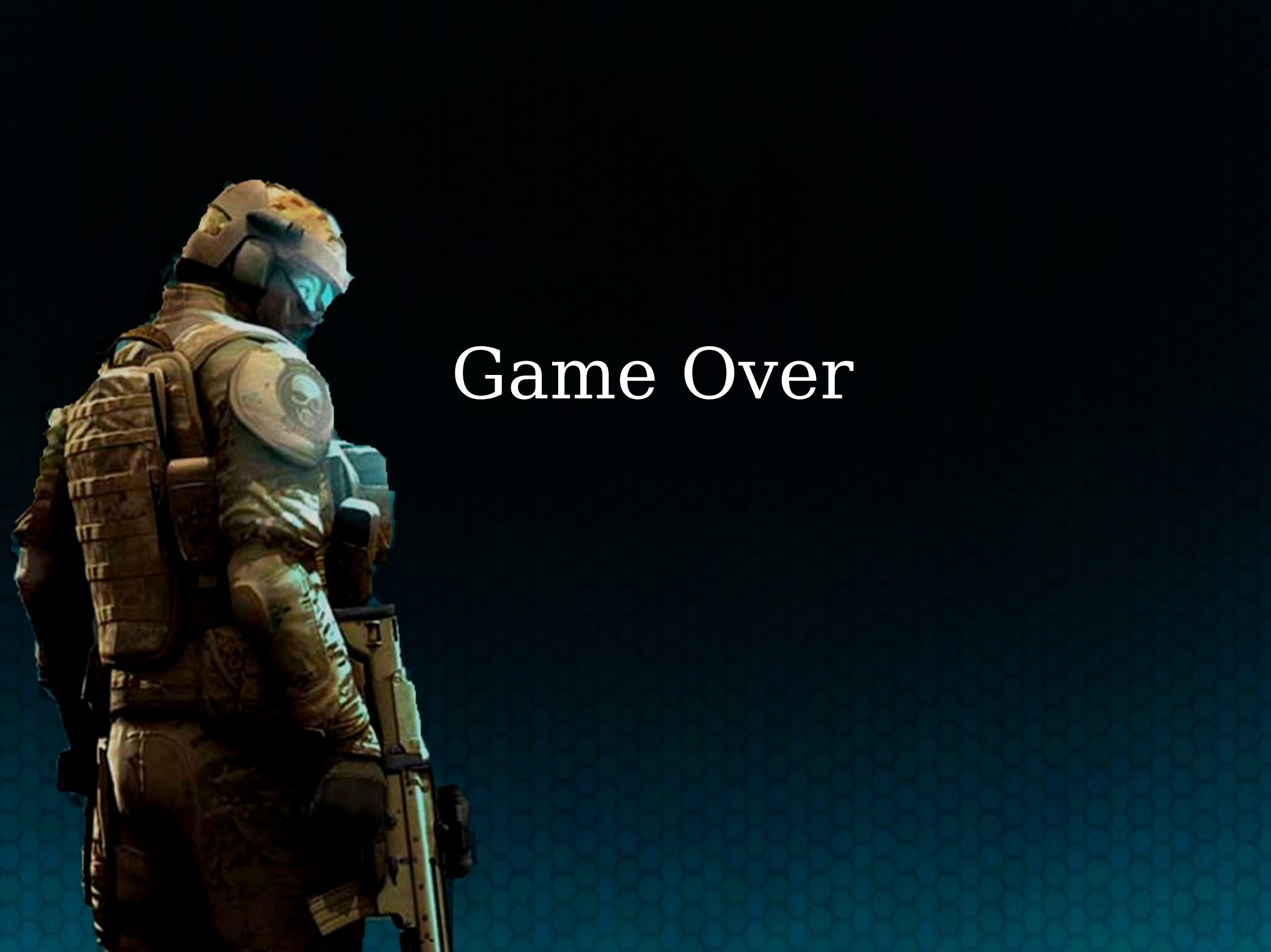


Fingerprinting

- LLDP
- Scapy/P0f
- PADS
- NetworkMiner
- Satori

Demo

- VRRP Takeover
- OSPF Route Manipulation


Game Over

Summary

- LLDP reveals the L2 Topology
- OSPF reveals the L3 Topology
- Hostile take-overs in VRRP
- OSPF Route-manipulation

Conclusions

- Use strong authentication
  - Use long passwords
  - Time to replace MD5
- Monitor logs

Thank You

- Berne Campbell
  - berne.campbell@gmail.com

Appendix

References

- IEEE 802.1AB-2005
- RFC 2328 OSPF
- RFC 3768 VRRP

References (2)

- Feiyi Wang and S. Felix Wu, "On the Vulnerabilities and Protection of OSPF Routing Protocols," In IEEE 7th International Conference on Computer Communication and Network (IC3N), October 1998 http://www.cs.ucsb.edu/~seclab/project

References (3)

- Emanuele Jones and Olivier Le Moigne, "OSPF Security Vulnerabilities Analysis," draft-ietf-rpsec-ospfvuln-02.txt, 16 June 2006.
- A. Babir, S. Murphy, Y. Yang, “Generic Threats to Routing Protocols”, draft-ietf-rpsec-routing-threats-07, 25 October 2004

References (4)

- Ayikudy Srikanth; Adnan Onart, “VRRP: Increasing Reliability and Failover with the Virtual Router Redundance Protocol”, ISBN-13 978-0-201-71500-2

Tools

- Scapy
  - http://trac.secdev.org/scapy/wiki
- Scapy_OSPF
  - http://trac.secdev.org/scapy/wiki/OSPF
- Scapy VRRP
  - http://trac.secdev.org/scapy/ticket/60
- P0f
  - http://lcamtuf.coredump.cx/p0f.shtml

Tools (2)

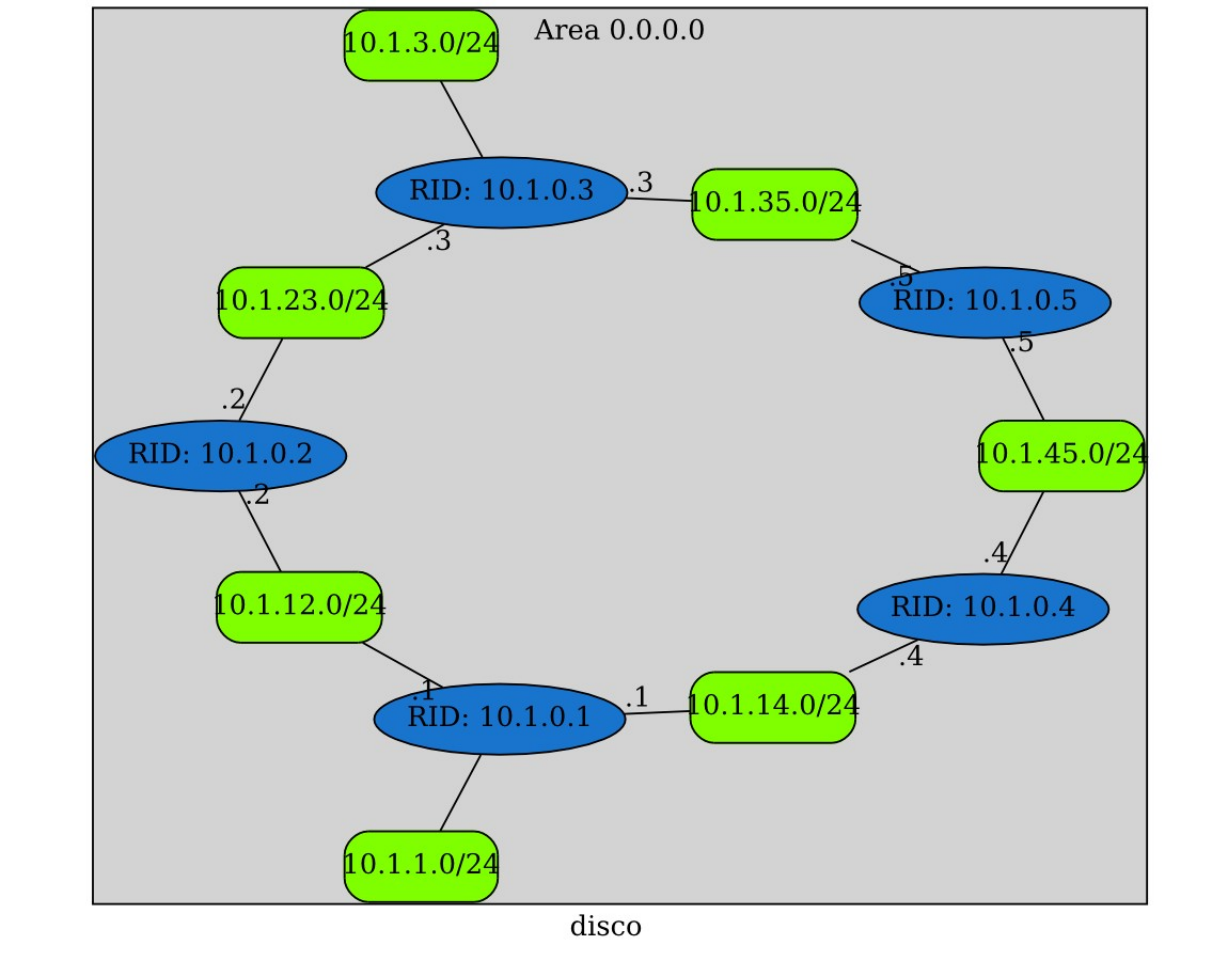
- Vyatta
  - http://www.vyatta.org/

Special Thanks

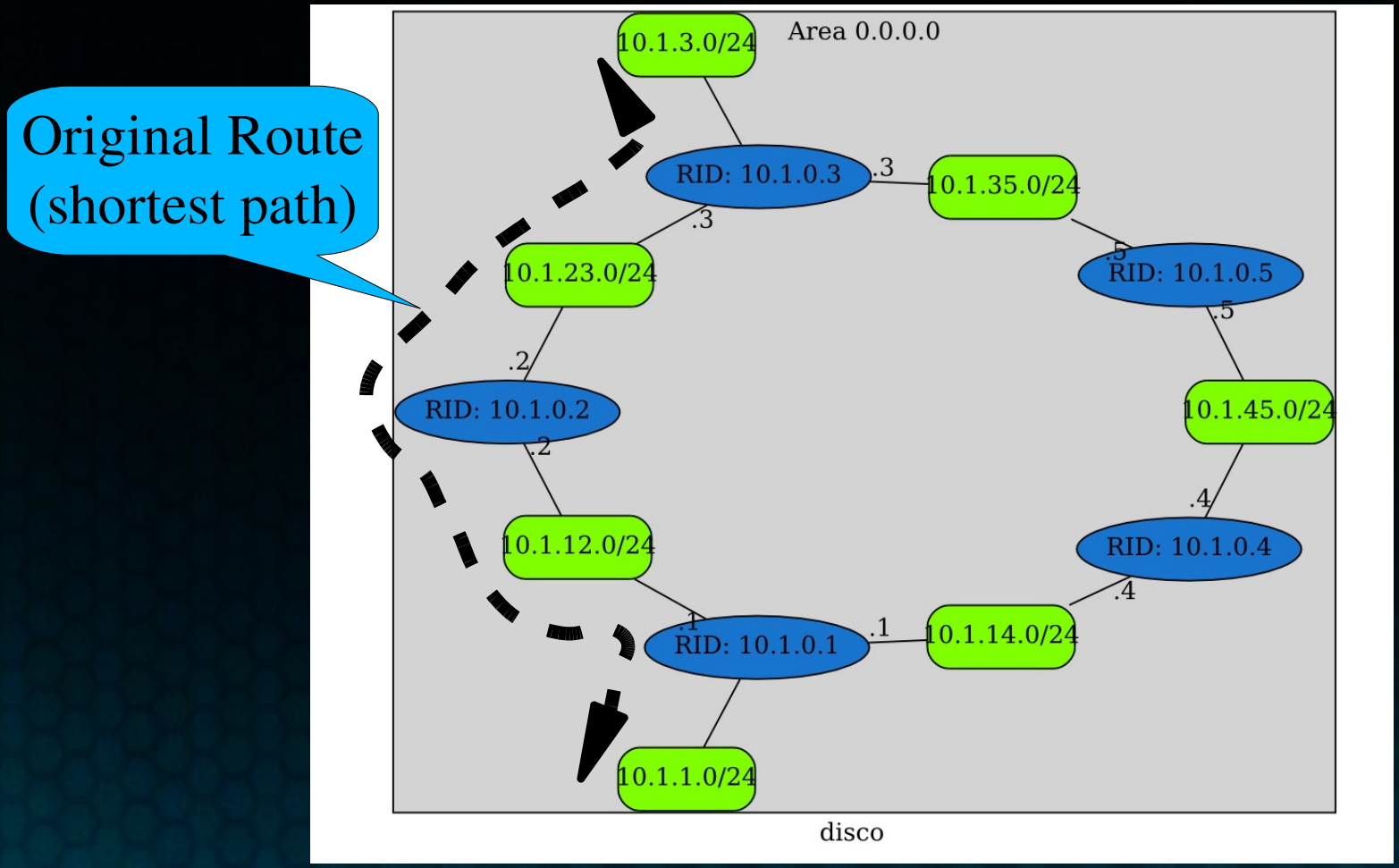
- telljoolz
- pemky
- Ruxcon Organisers and Staff

Removed Slides

Demo OSPF Topology Discovery

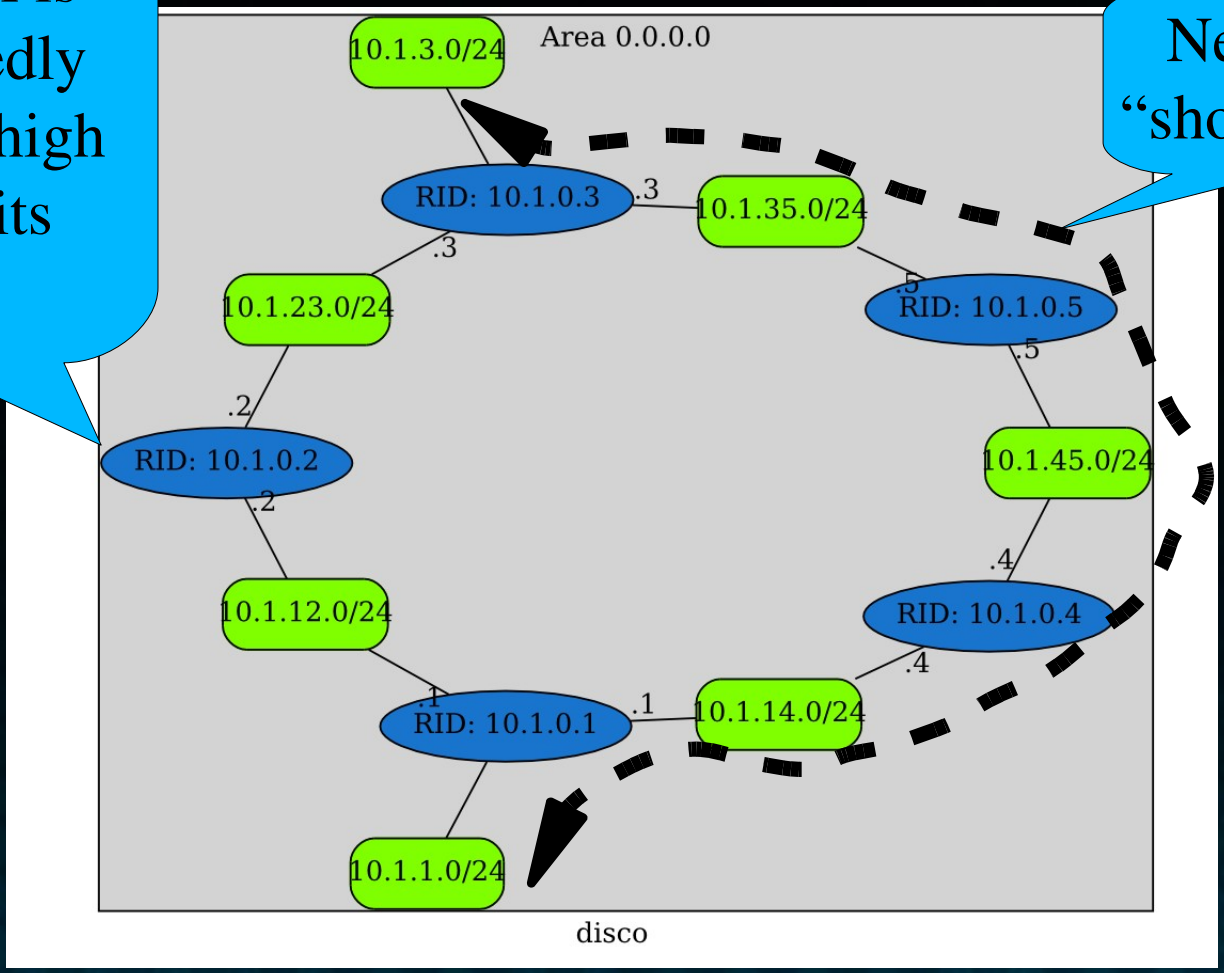


Demo ghOSPF Re-route



Demo ghOSPF Re-route

Router's LSA is being repeatedly spoofed with high metrics for its interfaces



New Route “shortest path”

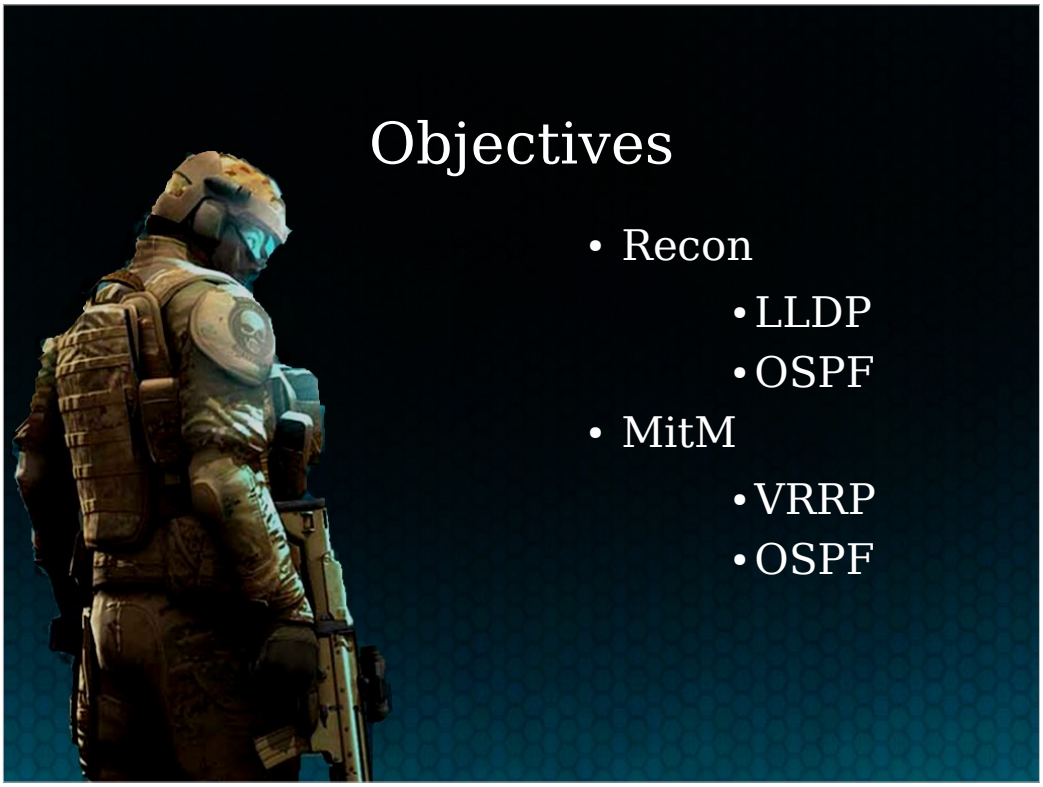
Vyatta

- Open source Router
- Based off Debian Lenny and Quagga


GHOST
RECON


Why?
• Network Security
• Information Gathering
• Eavesdropping
• MitM
• Invisibility

Who needs it?


Objectives
• Recon
• LLDP
• OSPF
• MitM
• VRRP
• OSPF


Recon
• LLDP
• OSPF

Link Layer Discovery Protocol

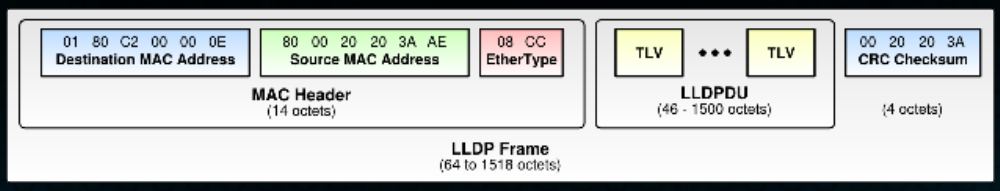
- IEEE 802.1AB-2005
- Vendor Neutral
- Similar functionality to CDP, EDP, NDP
- Layer 2
- Multicast MAC 01:80:c2:00:00:0e

LLDP

- TLV based protocol
- Info includes: -
    - System name & desc
    - Port name & desc
    - VLAN
    - IP Management address

LLDP Frame

- Click to add an outline

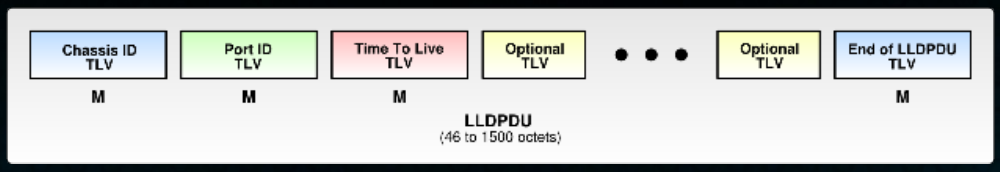


LLDP TLVs

- Mandatory TLVs: -
  - Chassis ID
  - Port ID
  - TTL
  - End of LLDPDU TLV
- Optional TLVs between TTL and EoL

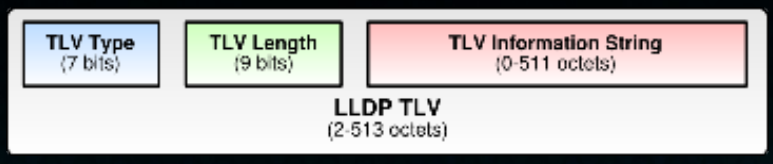
LLDPDU

- Click to add an outline



LLDP TLV

- Click to add an outline



LLDP Topology Discovery

- SNMP
- Local
    - LLDPD
- Multiple Hops
    - NetDisco
    - Wiremaps

Open Shortest Path First

- Routing Protocol
  - RFC 2328
  - Link State
- Similar to IS-IS
- Simple Authentication
  - Plain-text Password
  - MD5

Link State routing protocols were born out of ARPANET

OSPF is ~ 20 years old

The maths its based off (Dijkstra's Algorithm) is 50 years old

MD5 Authentcation is not HMAC-MD5

MAC = MD5 (OSPF || Key)

Note: key is padded to 16 bytes with nulls

OSPF Hierarchy

- Areas
  - Backbone == 0.0.0.0
  - Non-backbone != 0.0.0.0
  - All areas connected to backbone
- Routers
  - Internal Routers (IRs)
  - Area Border Routers (ABRs)
  - Autonomous System Border Routers (ASBRs)

OSPF

OSPF Link State

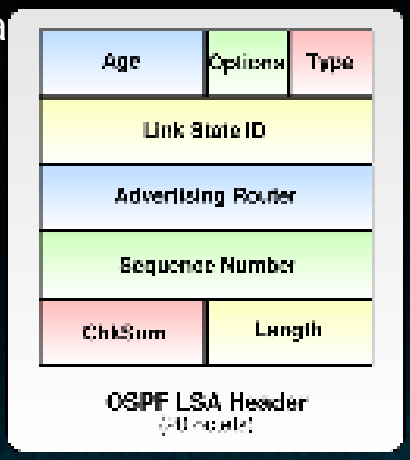
- Link State Database
  - Made up of LSAs
- Link State Advertisements (LSAs)
  - Type
  - ID
  - Advertising Router
  - Instance (Seq, Chksum, Age)

OSPF LSAs

- LSA Types
  - Router LSAs
  - Network LSAs
  - Summary LSAs
  - ASBR Summary LSAs
  - External LSAs

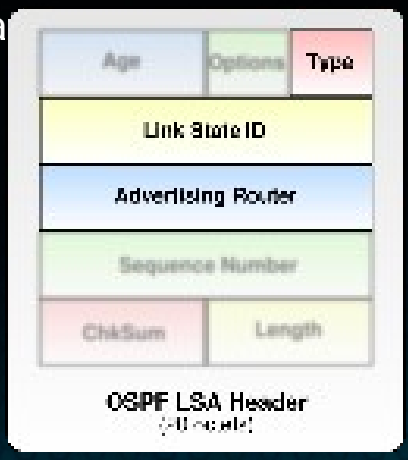
OSPF LSA Header

- Click to a



OSPF LSA Lookup

- Click to a

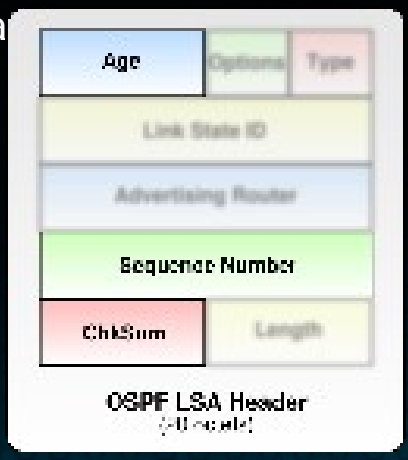


Type, Link State ID and Advertising Router are the three fields that are used to look up LSAs

If a router receives a request for a Type, ID, AdRouter tuple that does not exist in its database it will reset the neighborship. So to be stealthy when spoofing LS Requests make sure you look up known Type, ID, AdRouter tuples.

OSPF LSA Instance

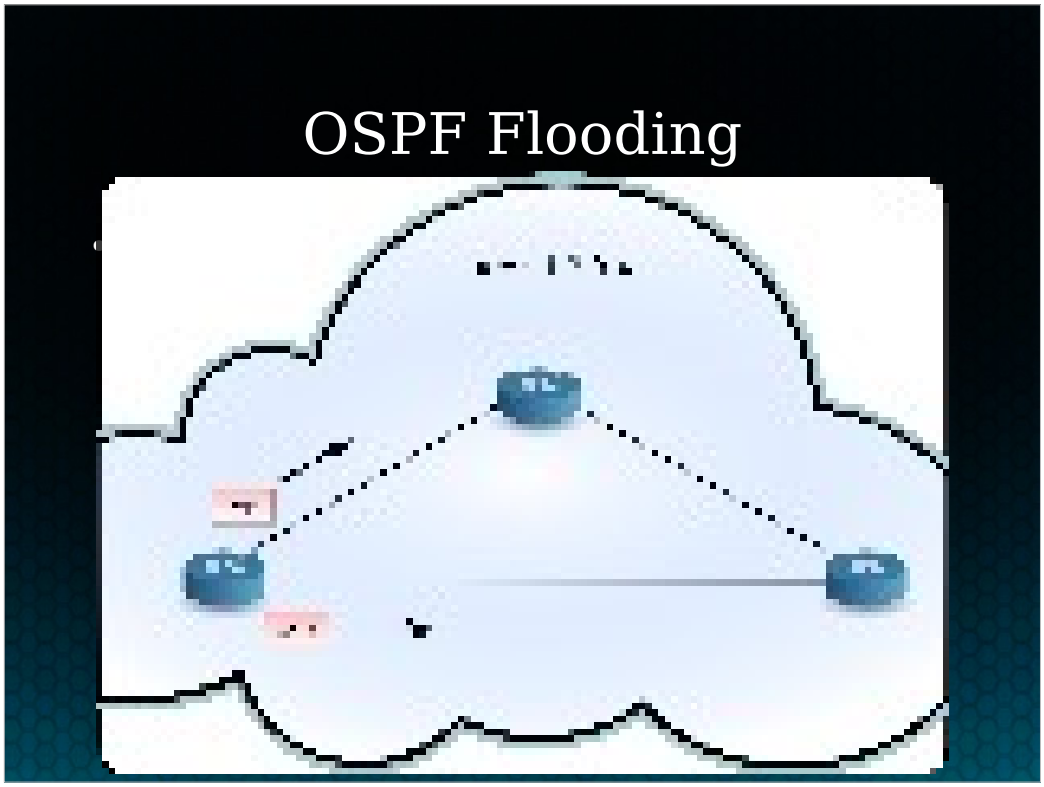
- Click to a



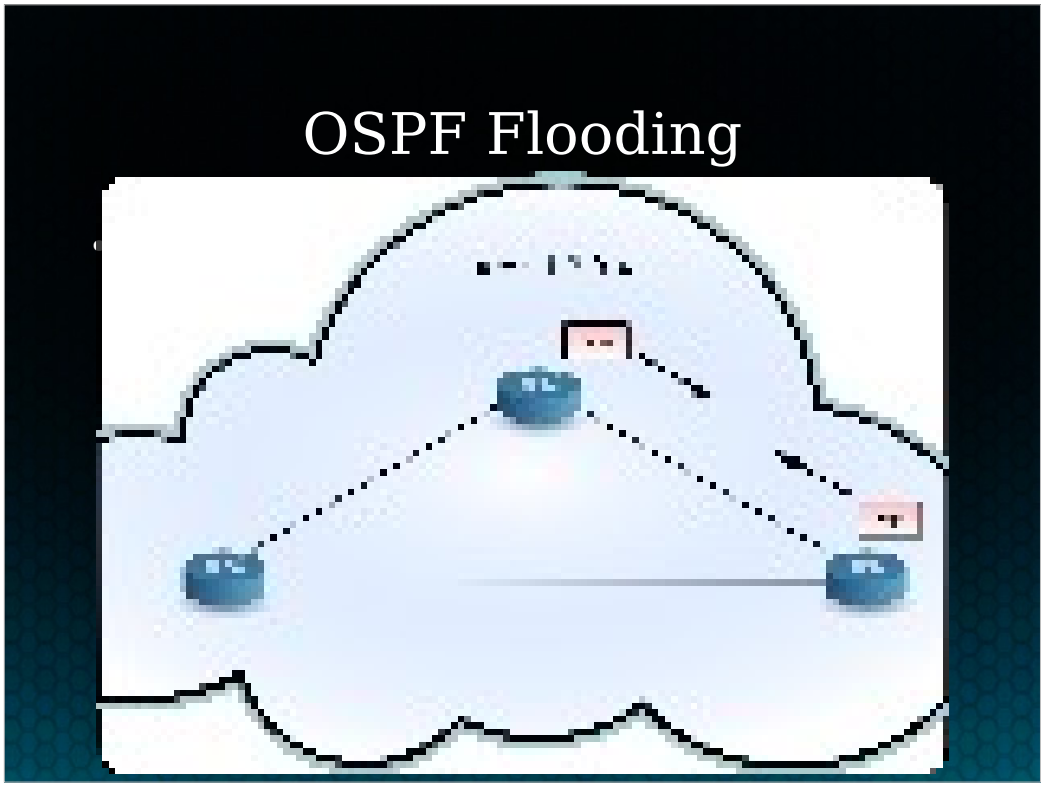
Age, Sequence Number and ChkSum are the three fields used to determine the which instance of an LSA is the most recent.

OSPF Neighbourships

- Adjacent Routers form neighbourships
- Exchange link state information
- Flood updates
- Synchronized LS Databases



Step 1: An OSPF Router floods updates to all of its neighbours (after a change in the topology for example).



Step 2: The receiving OSPF routers then flood the update to neighbours and so on throughout the network.

OSPF Broadcast Networks

- Broadcast networks
  - Multicast 224.0.0.5 and 224.0.0.6
  - Designated Router (DR)
  - Backup Designated Router (BDR)
  - DR originates Network LSA

Obviously since OSPF uses multicast, ARP Poisoning tricks cannot be used against it.

OSPF Topology Discovery

- Passive
  - LSRefreshTime (30 Mins)
- Active
  - Subvert Router
  - Rouge Router
  - Spoof LSA Requests

Juniper routers actually refresh at 50 minutes, as an optimization (although this technically makes them non-standard).

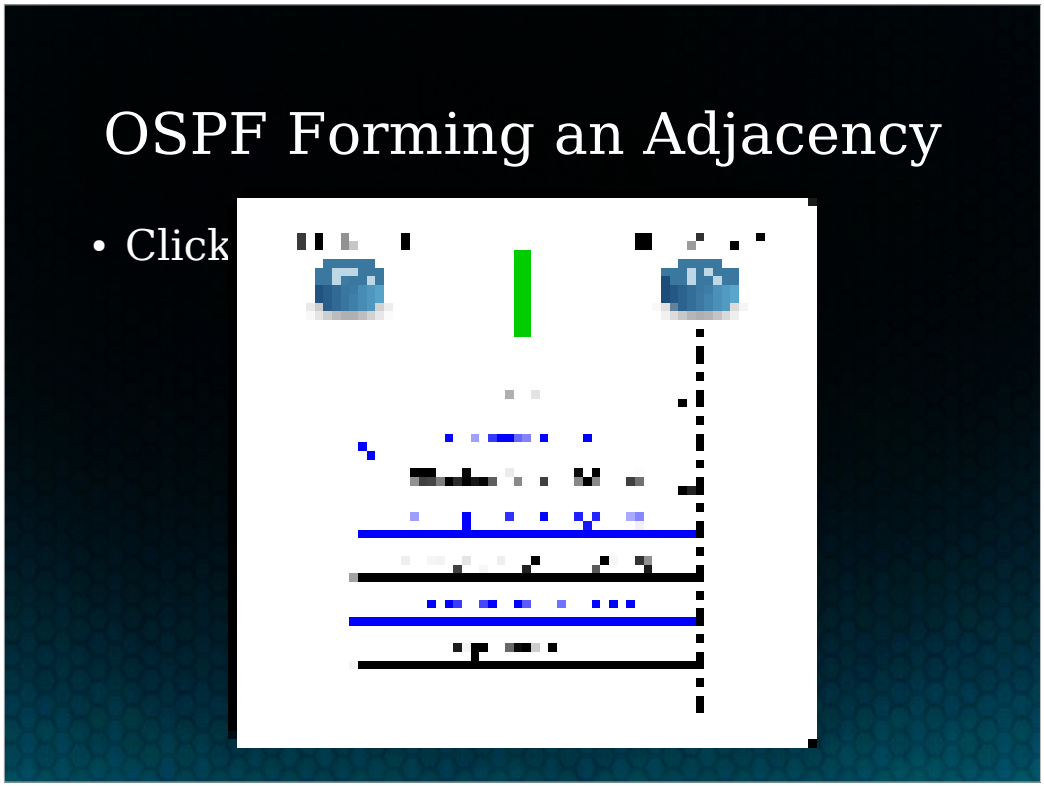
OSPF Active Topology Discovery

- Router LSAs
  - ID == Advertising Router
- Network LSAs
  - ID == DR's IP
  - Adv Rtr == DR RID
- Limitation with BDR
  - Unknown DR RID

To lookup a router LSA you only need the ID/Adrouter as they are both the same, and of course the type is “router”.

To look up a Network LSA you need to know the DR's IP, and the DR's Router ID.

Spoofing LS Requests to get the LSAs based off Type, ID, Adrouter tuples that have been gleaned from passively monitoring the network will allow topology discovery with the limitation that when hitting a BDR, you will know the DR's IP, but not the DR's RID, and therefore you will be unable to make a valid request for the Network LSA of that network until the DR's RID is learned.



This is a simplified diagram of the OSPF Adjacency procedure.

First the routers seach each others RID in each others Hellos. This means they have bidirectional communication.

They then describe each others databases to each other.

Then they make LS Request of missing LSAs.

Add-on to scapy_ospf add-on
Passive: -
Slower
Full topology after ~LSRefreshTime
(30mins Standard – Juniper 50mins)
More stealthy

Active: -
Quicker
Less stealthy

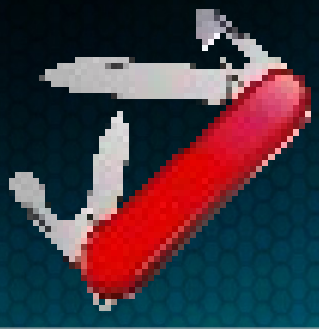
Spoof LS Requests
Limitations on discovery (DR/BDR)

Kill a neighbourship
Noisy - logs

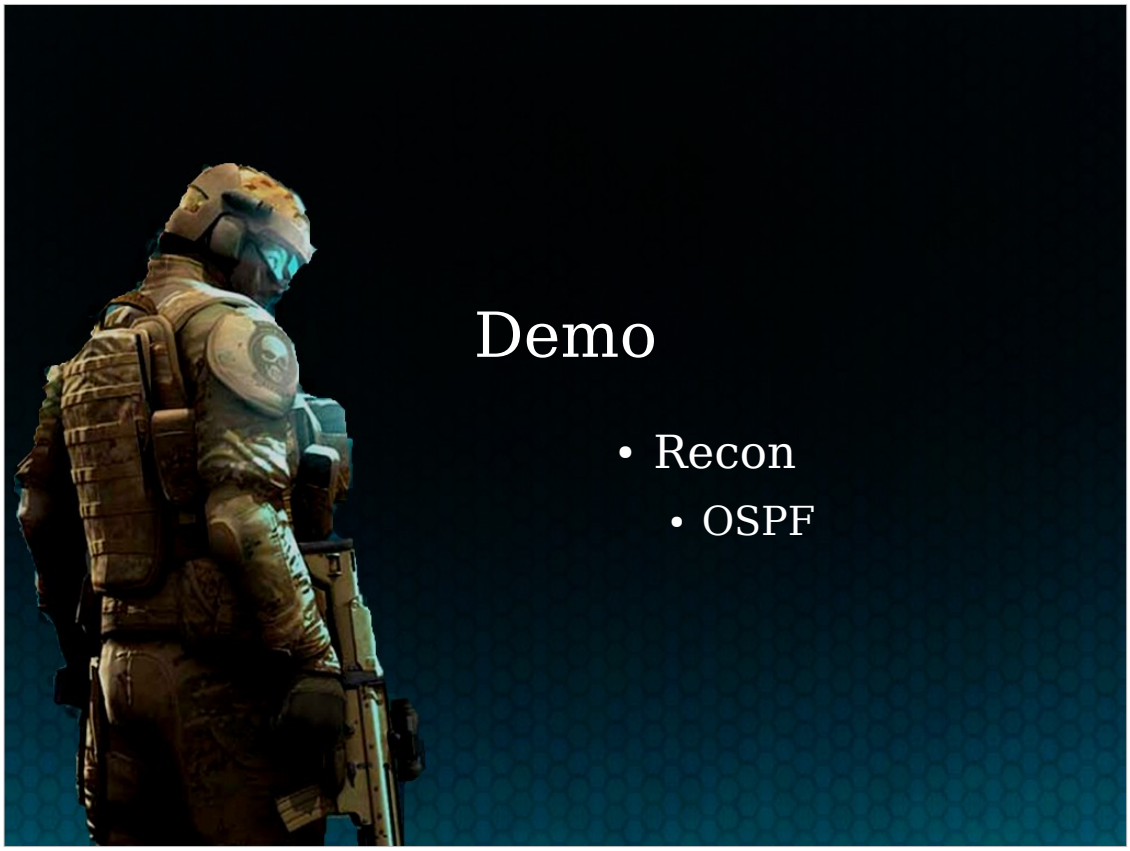
Phantom Router
Noisy – logs – stop mid-way to reduce logs

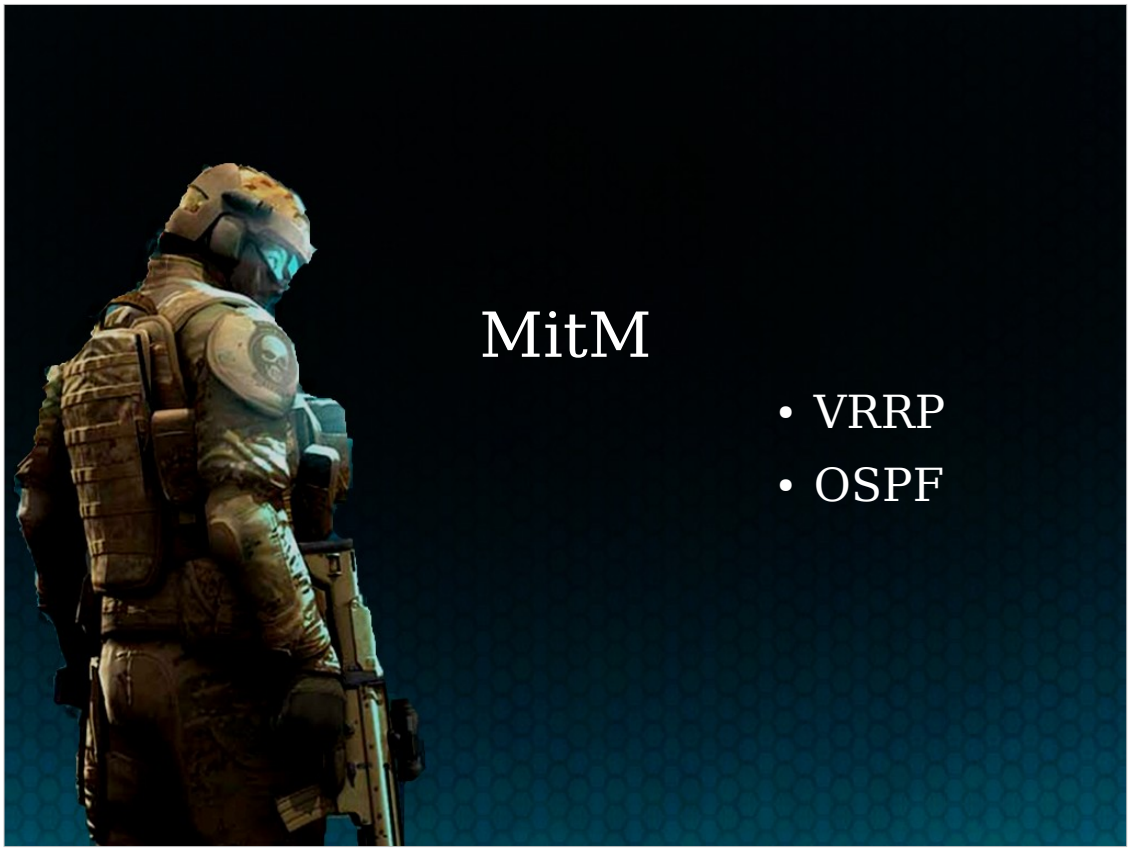
Scapy

- Python Packet Manipulation Tool
- Philippe Biondi
- Decodes rather than interprets
- Replaces numerous tools
- Combine functionality
- Add-ons



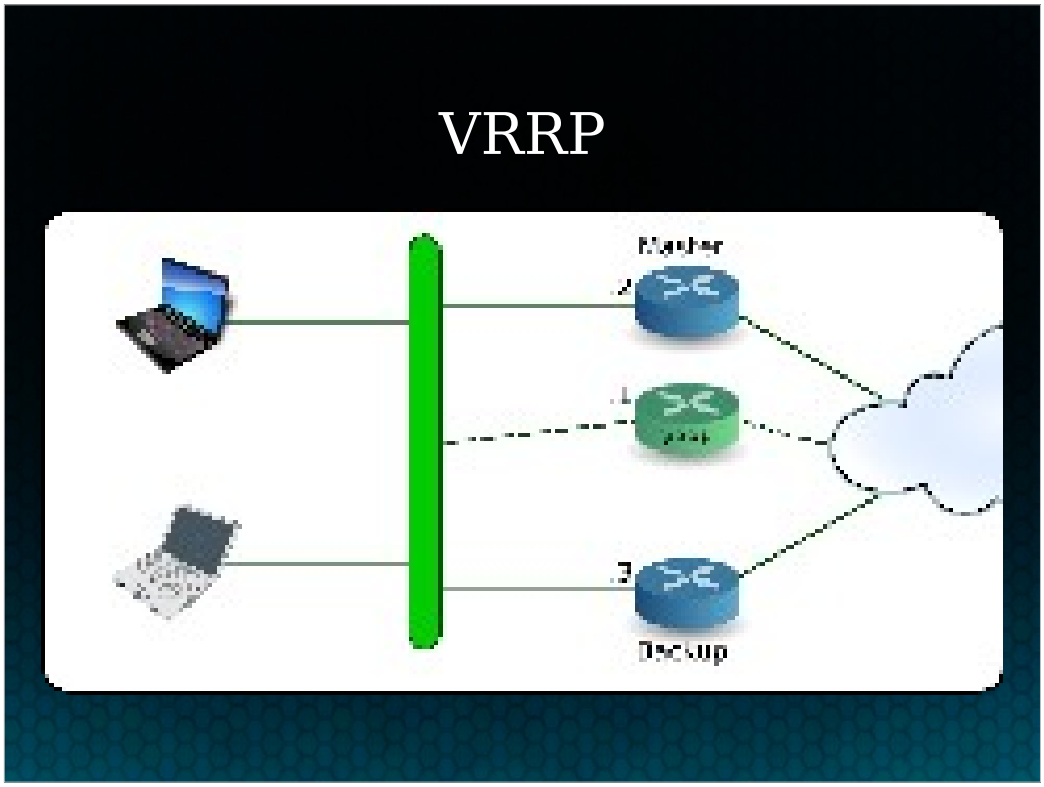
http://www.secdev.org/projects/scapy/


Demo
• Recon
• OSPF

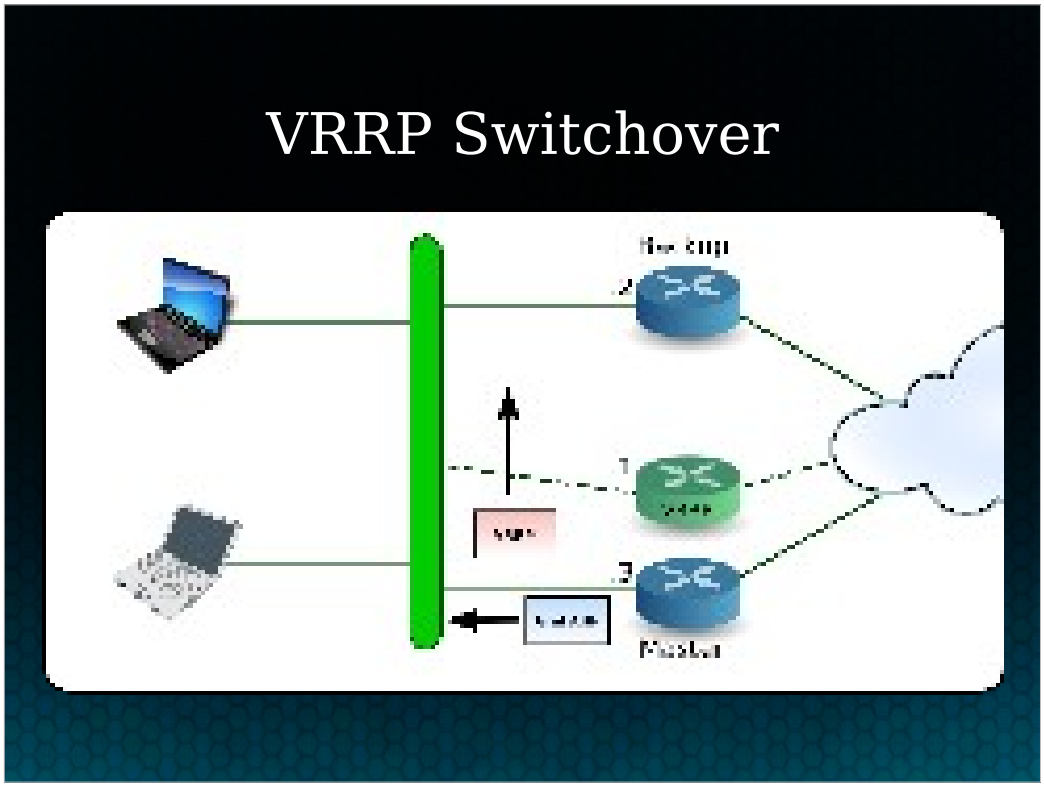

MitM
• VRRP
• OSPF

Virtual Router Redundancy Protocol

- First Hop Redundancy
- Provides Fault Tolerance
- Based off Cisco's HSRP
- Layer 3
- Standardized - RFC 3768
- Current version 2
- Uses Gratuitous ARP with BIA MAC



In this example, the two routers are in the one VRRP group with a floating virtual IP. The two routers cooperate to create a Virtual Router. If the master, who is currently performing the actions of the virtual router, should fail then the Backup will become master and start to perform the actions of the virtual router. The virtual router therefore has higher availablity due to the redundancy. The virtual IP is typically used as a default route for hosts.



On a switch-over the Backup sends out a VRRP Announcement and gratuituous ARPs for the Virtual IP Address(es).

VRRP Security

- TTL 255 (directly connected)
- Authentication
  - None
  - Plaintext password
  - MD5 PSK (Non-standard)
  - IPSEC AH
    - Truncated MD5 HMAC
    - Not supported by all implementations

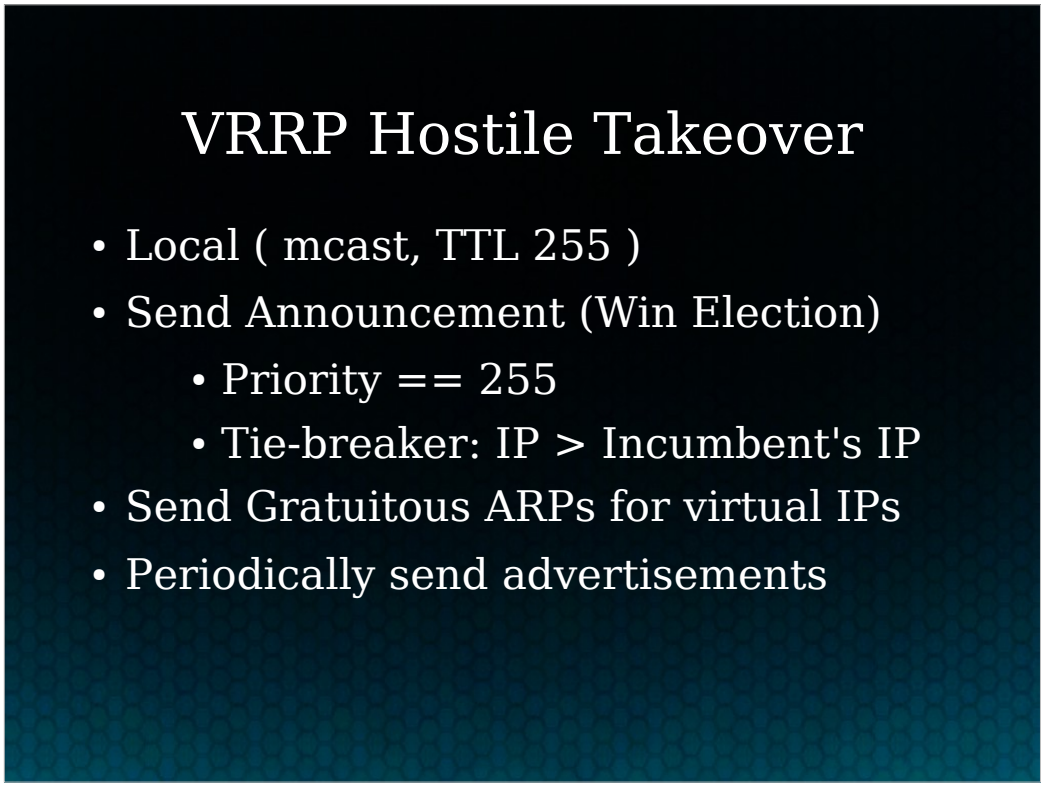
As the TTL must be 255, remote hosts trying to manipulate VRRP will fail as the TTL will be decremented at each hop. Only local hosts will be able to attack VRRP.

VRRP Pre-empting

- Default Priority 100
- Priority 255 reserved for Owner
- Pre-empting is typical
    - Owner always pre-empts regardless of pre-empt setting
    - Pre-empt on by default

VRRP Switchover

- New-Contestent pips Incumbent Master iff: -
    - NC's Priority > IM's Priority
- Tie-breaker: -
    - NC's Primary IP > IM's Primary IP



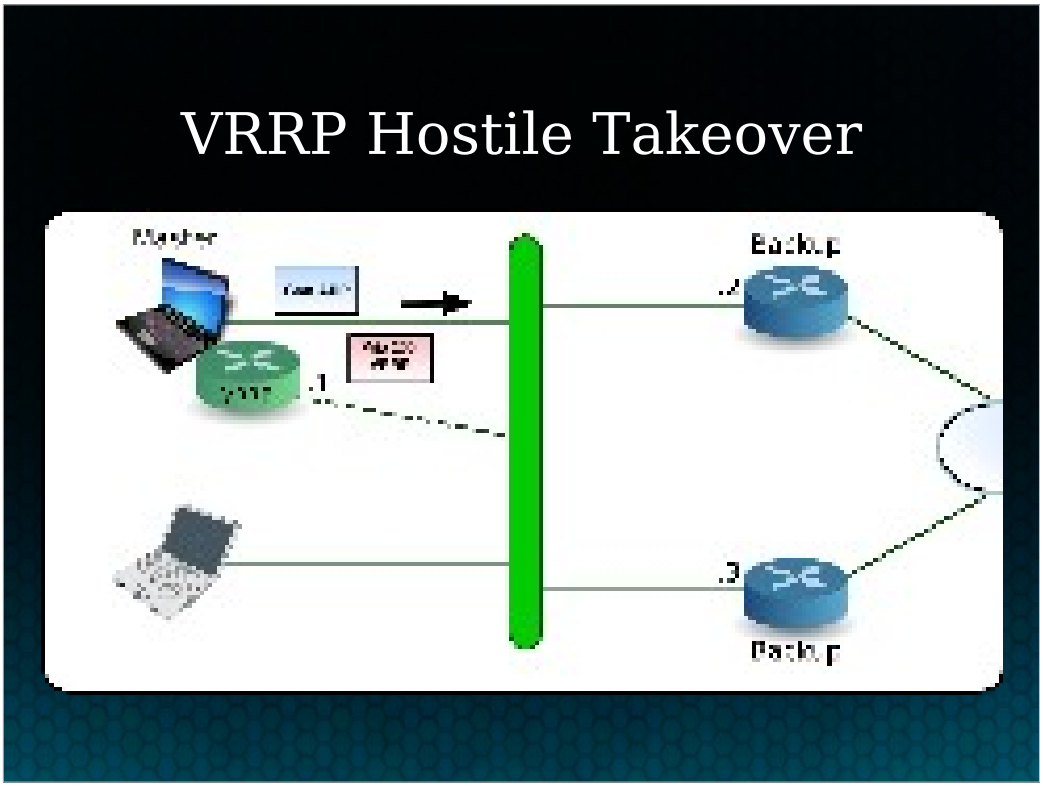
Local

- IP DST = 224.0.0.18
- IP TTL == 225

VRRP Version 2

Type 1 Advertisement – The only type.

VRRP Hostile Takeover

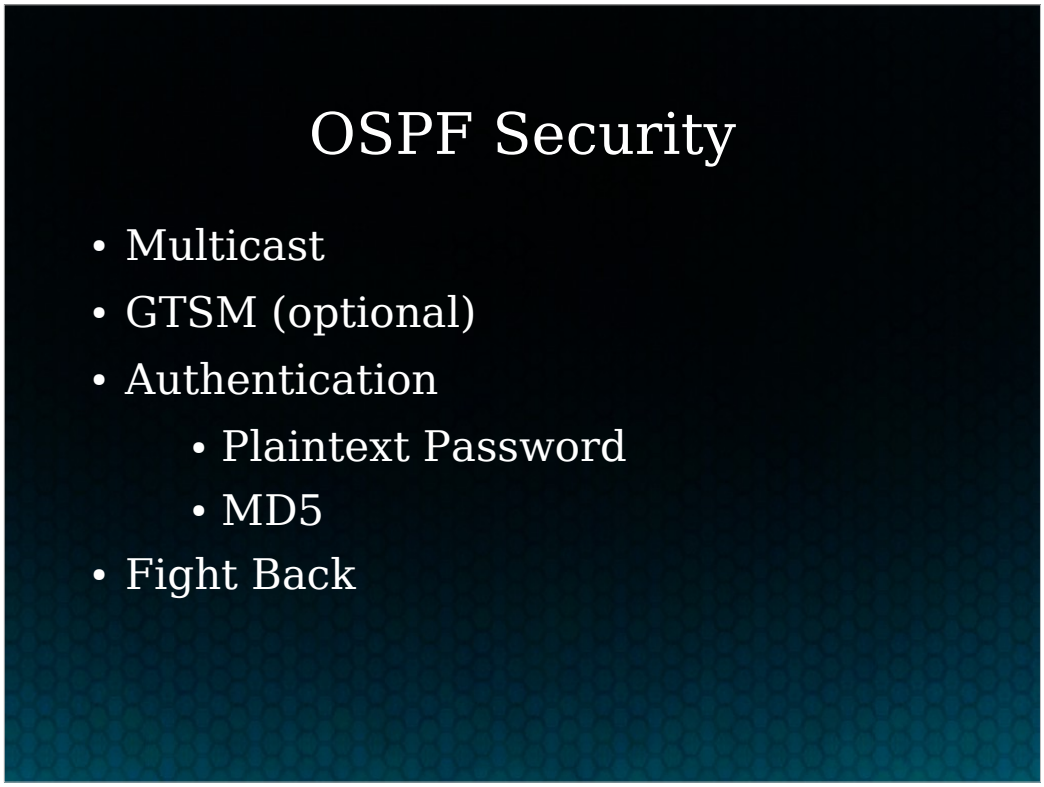


A malicous host could perform a hostile take over of the VRRP group by sending a VRRP announcement with a higher priority (for example 255 – the highest) and gratuitous ARPs for the virtual IP address(es).

If the incumbent master has a priority of 255 the malicious host could use a higher primary IP to win the tie-breaker.

OSPF attacks may come from a legitimate that is compromised or from a network segment with OSPF router(s) running on it that is compromised.

One existing tool to attack OSPF is the OSPF Attack Shell by GomoR. And now there is also ghOSPF.



Routing security is a hard problem: -

- Highly Distributed
  - Routing is a cooperative process, with many nodes involved
- Highly Dynamic
- Nodes need to trust each other
- Protocol must be secure
  - Protocol flaw-free
  - Implementation Bug-free
  - Authentication

- MD5 Authentication is not HMAC-MD5
  - MAC = MD5 (OSPF || Key)

- IPsec/HMAC-SHA1 is on the road-map (haha)
  - draft-gupta-ospf-ospfv2-sec-00
  - draft-ietf-ospf-hmac-sha-03.txt

One additional feature of ghOSPF is Route Manipulation / Injection.

OSPF Route Manipulation

- Routing ← SPF ← LSDB ← LSAs
- Intra > Inter > E1 > E2
- LSA's metrics – cost
- Partitioned LSAs won't go into SPF
- Must spoof LSA(s)
    - Must Fight Fightback

The routing table is derived from the results of Shortest Path First algorithm applied to the Link State Database. The LSDB contains all the current LSAs.

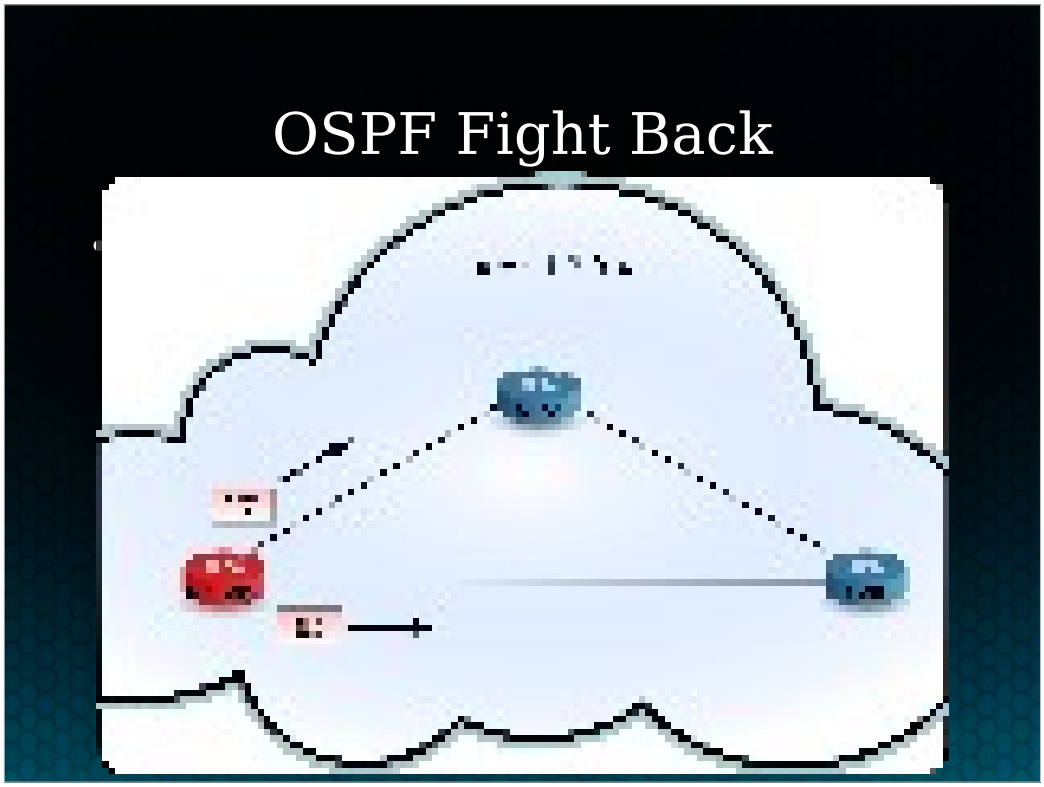
Intra-Area routes are prefered over Inter-Area routes, which are prefered over external routes. External Type 1 routes are prefered over External Type 2 routes.

(Maliciously injected) LSAs that are partitioned from the area will not go into the SPF and therefore the routing table. Therefore we must spoof LSA(s) to manipulate the routing table – unless you are advertising new networks with a phantom router.

If spoofing existing LSAs then you must fight fight back from the legit originating router.

OSPF Fight Back

- Router receives “wrong” LSA
  - Same Advertising Router ID
  - Wrong details though
- Originates new LSA
  - Correct details
  - Newer Seq



The malicious router, Mallory, is sending LS Updates with that contain a spoofed LSA purporting to be originated by the router Bob.

Alice when receiving the new “Bob” LSA will install it and flood it as per normal, completely unaware of any nefarious activity.

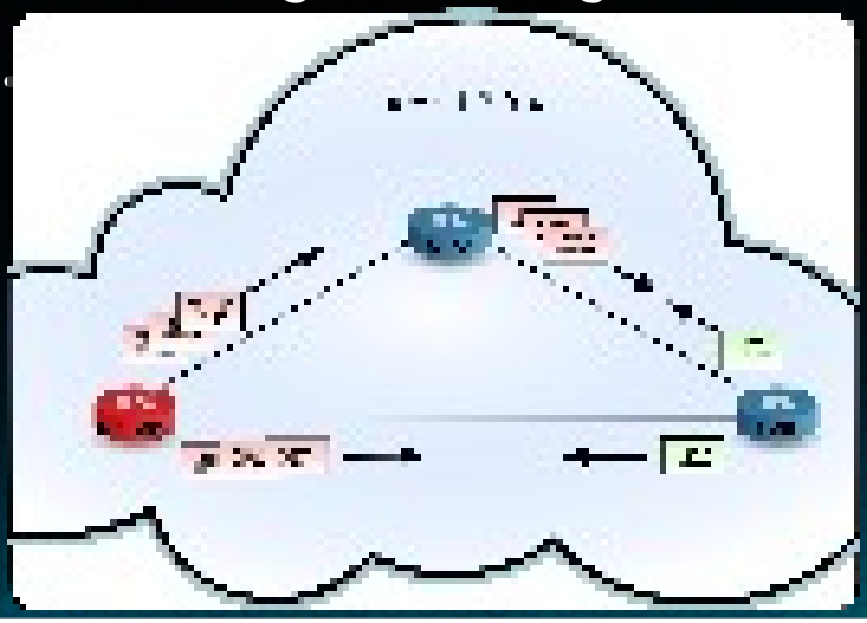
Bob when receiving the new “Bob” LSA however will originate a new update with the correct information. This is termed fight back.

Defeating OSPF Fight Back

- MinLSInterval
  - 5 seconds
  - Min time before originating LSA
- MinLSArrival
  - 1 second
  - Min time before processing LSA
- Race condition
  - Transmit LSAs @ 1s with > Seq

In practice OSPF routers seem to breach the MinLSInterval when fighting back.

Defeating OSPF Fight Back



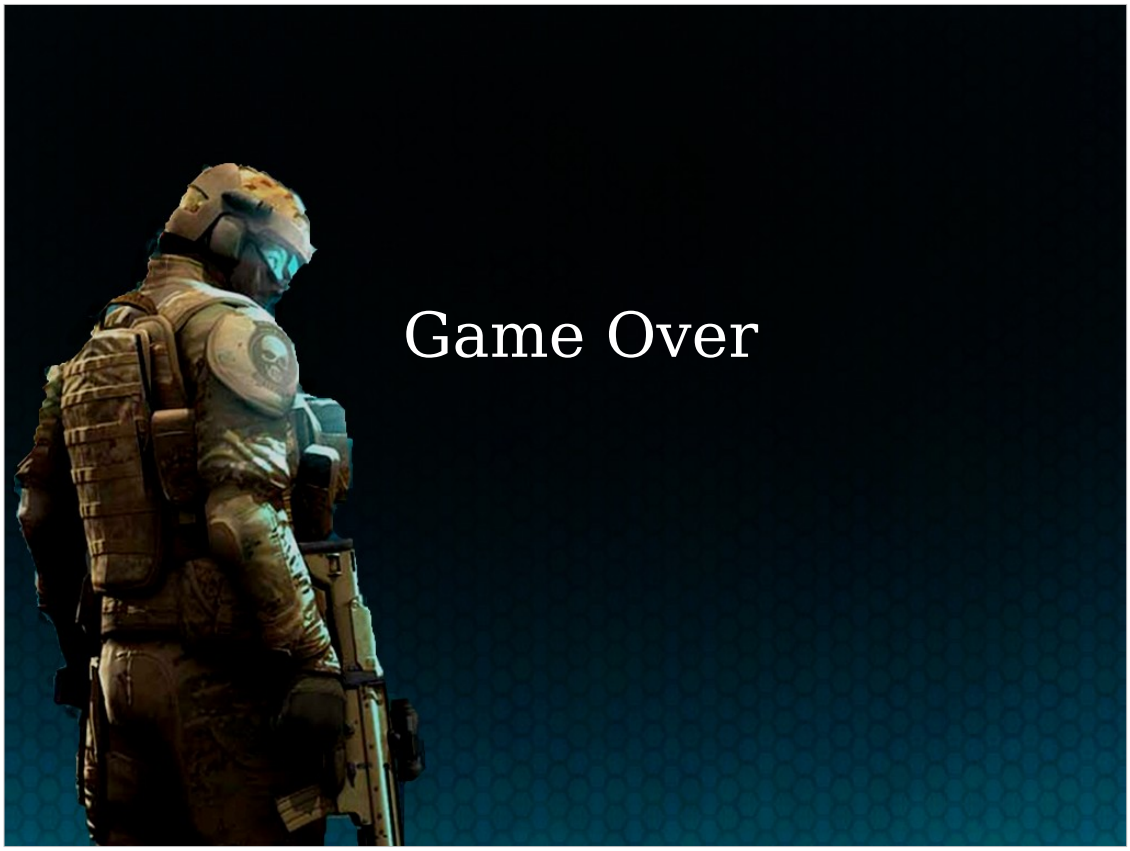
Fingerprinting

- LLDP
- Scapy/P0f
- PADS
- NetworkMiner
- Satori

LLDP obviously includes lots of information that can be very useful for topology discovery as well as information about the host.

Tools such as (scapy/)p0f, PADS, NetworkMiner, and Satori can be used to passively guestimate the OS and versions from (re-routed) traffic.


Demo
• VRRP Takeover
• OSPF Route Manipulation

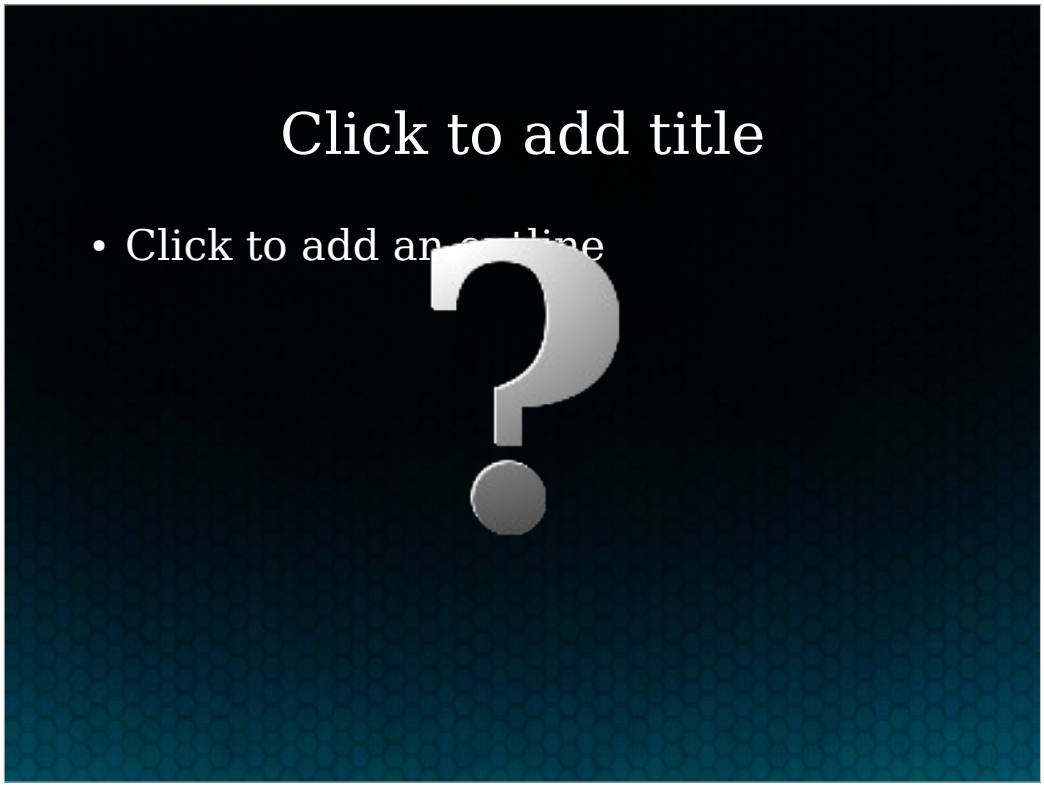

Game Over

Summary

- LLDP reveals the L2 Topology
- OSPF reveals the L3 Topology
- Hostile take-overs in VRRP
- OSPF Route-manipulation

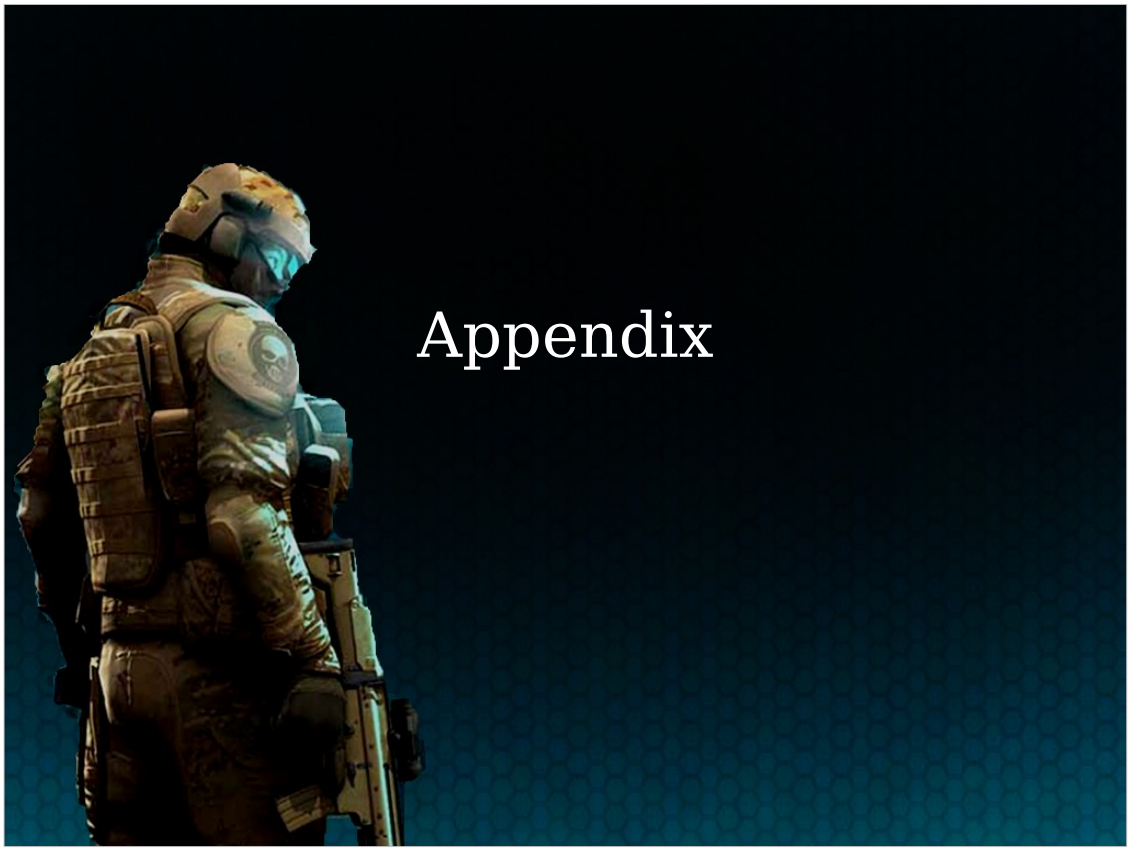
Conclusions

- Use strong authentication
  - Use long passwords
  - Time to replace MD5
- Monitor logs


Click to add title
• Click to add an outline

Thank You

- Berne Campbell
  - berne.campbell@gmail.com



Appendix

References

- IEEE 802.1AB-2005
- RFC 2328 OSPF
- RFC 3768 VRRP

References (2)

- Feiyi Wang and S. Felix Wu, "On the Vulnerabilities and Protection of OSPF Routing Protocols," In IEEE 7th International Conference on Computer Communication and Network (IC3N), October 1998 http://www.cs.ucsb.edu/~seclab/project

References (3)

- Emanuele Jones and Olivier Le Moigne, "OSPF Security Vulnerabilities Analysis," draft-ietf-rpsec-ospfvuln-02.txt, 16 June 2006.
- A. Babir, S. Murphy, Y. Yang, “Generic Threats to Routing Protocols”, draft-ietf-rpsec-routing-threats-07, 25 October 2004

References (4)

- Ayikudy Srikanth; Adnan Onart, “VRRP: Increasing Reliability and Failover with the Virtual Router Redundance Protocol”, ISBN-13 978-0-201-71500-2

Tools

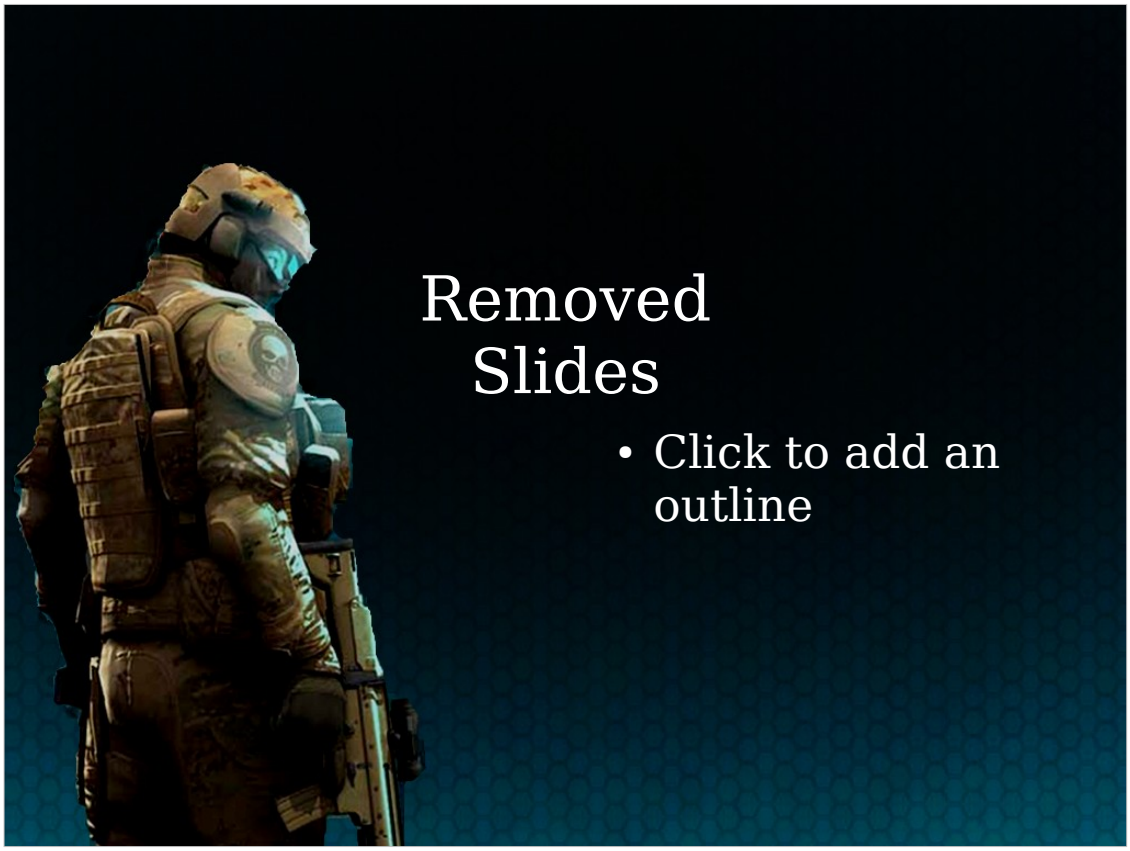
- Scapy
  - http://trac.secdev.org/scapy/wiki
- Scapy_OSPF
  - http://trac.secdev.org/scapy/wiki/OSPF
- Scapy VRRP
  - http://trac.secdev.org/scapy/ticket/60
- P0f
  - http://lcamtuf.coredump.cx/p0f.shtml

Tools (2)

- Vyatta
  - http://www.vyatta.org/

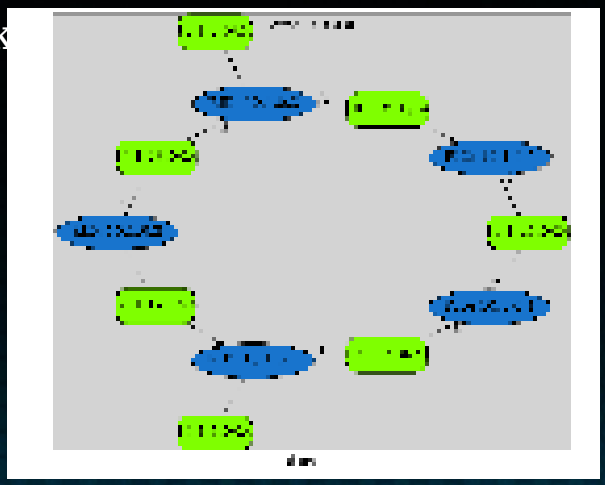
Special Thanks

- telljoolz
- pemky
- Ruxcon Organisers and Staff


Removed Slides
• Click to add an outline

Demo OSPF Topology Discovery

- Click



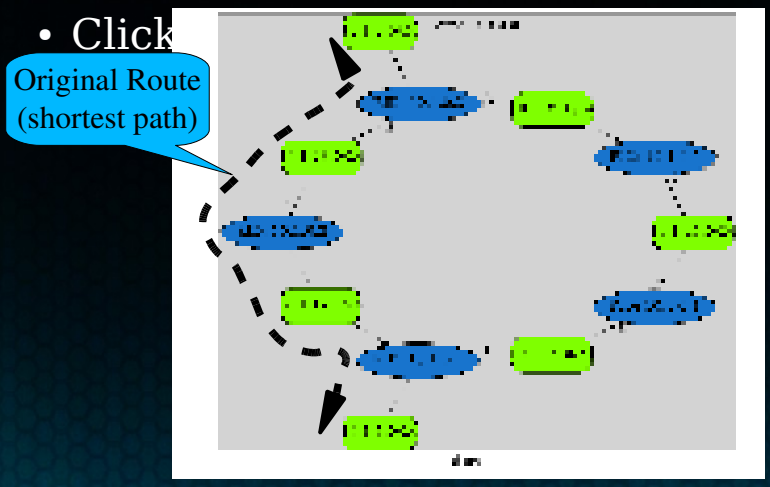
For those who missed the demo, this is what the results of ghOSPF's topology discovery look like.

In this demo ghOSPF was a host in the 10.1.45.0/24 network.

For time-constraint reasons the demo used the phantom router active attack

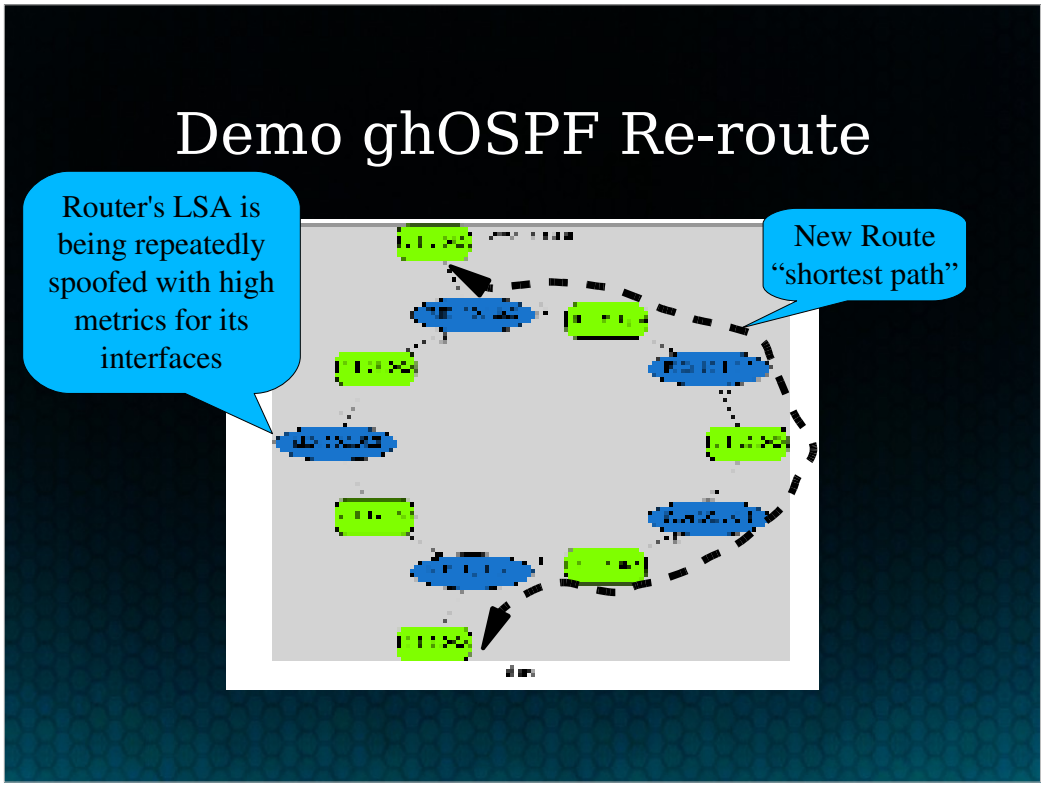
Demo ghOSPF Re-route

- Click



In the lab that I am using for the demo, all links are Ethernet, with the same default metric.

Traffic between the two stub networks 10.1.1.0/24 and 10.1.3.0/24 will take the left-hand-side, as it is the shortest-path.



GhOSPF running in the 10.1.45.0/24 subnet is repeatedly spoofing LS Updates with an LSA claiming to be a Router LSA for 10.1.0.2.

This spoofed LSA has much higher metrics than the legitimate Router LSA does.

Because the updates are repeatedly injected, the routers in the network install the spoofed LSA, and during their SPF calculations the right-hand-side is the shortest due to the left-hand-sides artificially high metrics.

Vyatta

- Open source Router
- Based off Debian Lenny and Quagga