OSPF Security: Attacks and Defenses

Manjul Khandelwal
(manjul@nivettisystems.com)
Ramakrishna DTV
(ramakrishnadtv@nivettisystems.com)

NIVETTI SYSTEMS

www.nivettisystems.com

Objective

Various attacks targeted at OSPF, their mitigations, and best practices for network based on OSPF

Focus: Important and recently reported attacks

Agenda

- Brief Introduction to OSPF
- Attackers, Goals and Consequences
- Various types of attacks and their mitigation
  - Remote attacks
  - Compromised router attacks
- Best practices
- Q&A

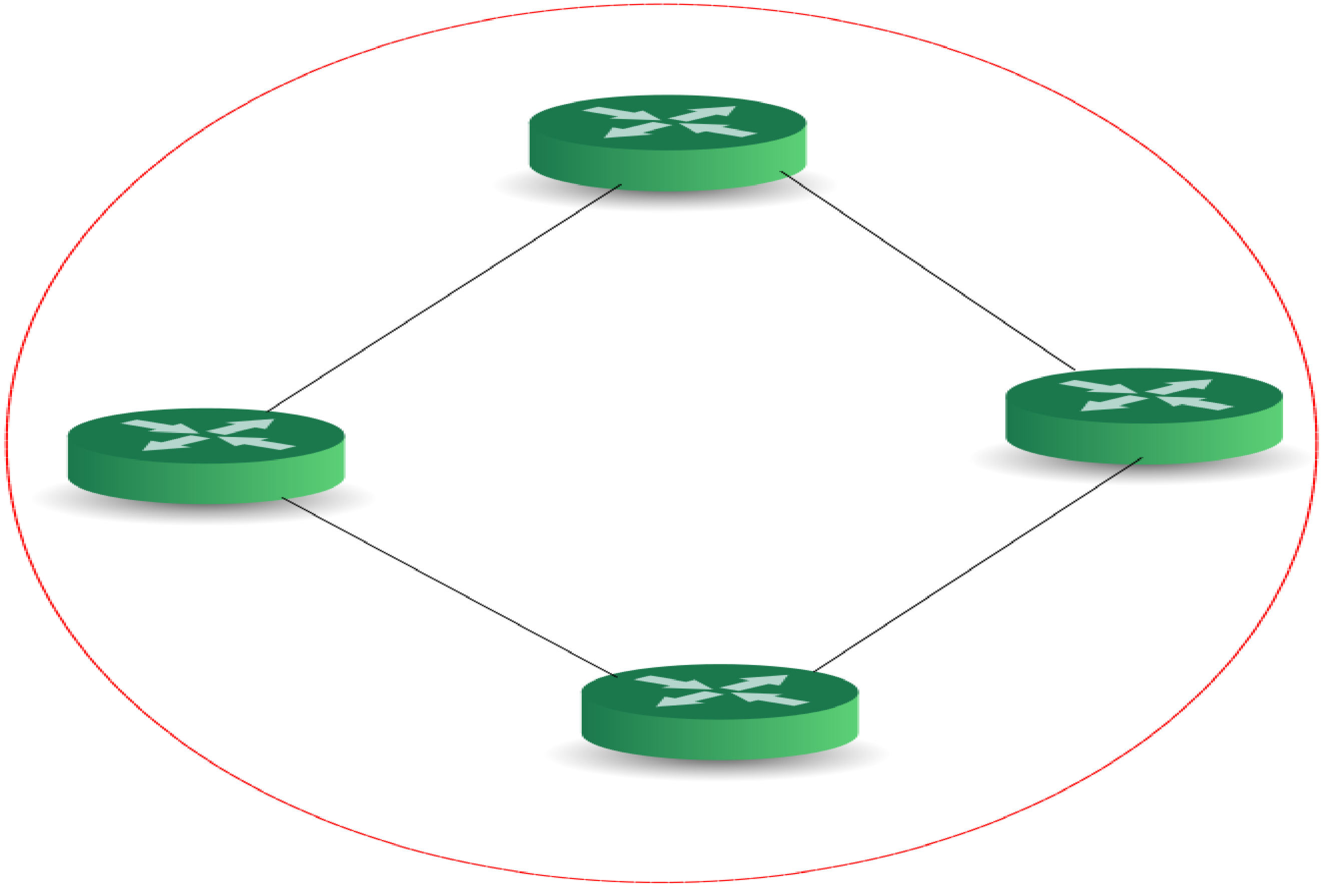
Agenda

- **Brief Introduction to OSPF**
- Attackers, Goals and Consequences
- Various types of attacks and their mitigation
  - Remote attacks
  - Compromised router attacks
- Best practices
- Q&A

OSPF

- IETF recommended standard for IGP
- Most commonly used IGP in enterprises and ISP networks

OSPF



Security strengths of OSPF

- Bidirectional links
- Cryptographic authentication
- Fight-back

Agenda

- Brief Introduction to OSPF
- **Attackers, Goals and Consequences**
- Various types of attacks and their mitigation
    - Remote attacks
    - Compromised router attacks
- Best practices
- Q&A

Goals of attackers

- Get access to needed information
  - But don't want to get detected
- Cause needed damage (DOS)

Consequences of attacks

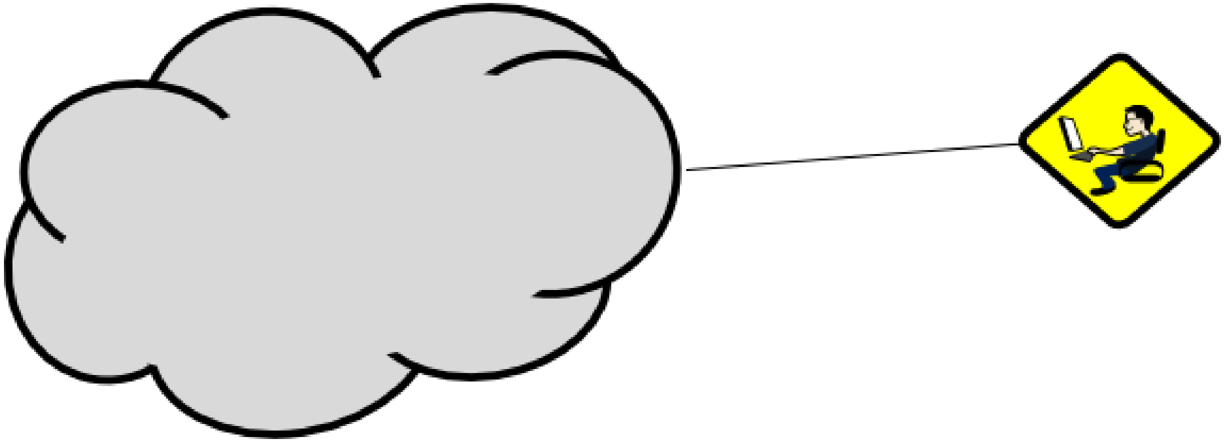
- Eavesdropping (Man-in-the-middle)
- Black holes
- Delay
- Loops
- Partition
- Congestion in the network
- Delayed or no convergence of routing tables
- Resource shortages on the routers etc
- Reported in [draft-ietf-rpsec-ospf-vuln-02]

Attackers

- Remote attackers
- Compromised routers

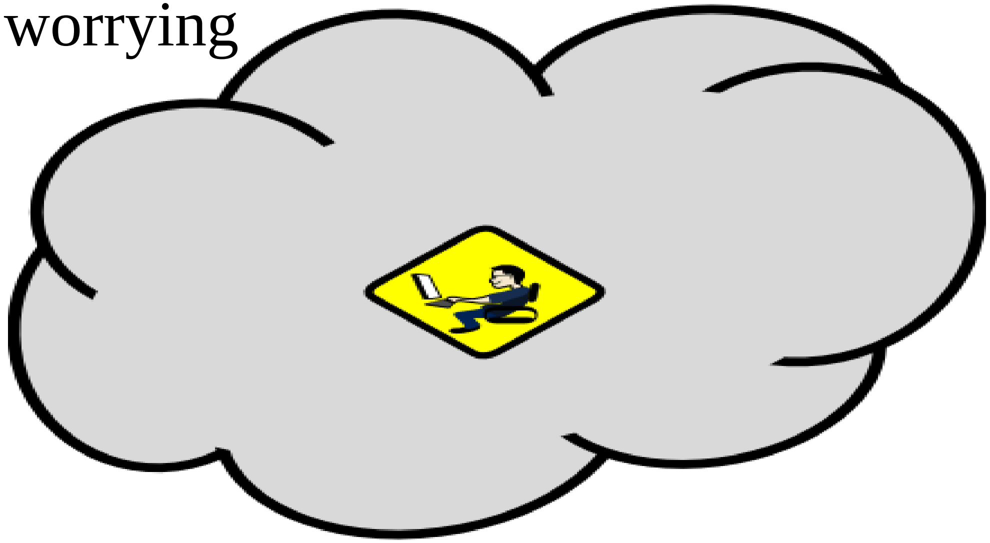
Remote Attackers

- Administrators consider this an important attack scenario
- Devote their attention to it
  - Implement mitigation measures



Compromised routers

- Many administrators do not devote attention to this attack and consider it as having negligible probability
- Some consider it as possible but do not worry about further consequences
  - Their logic: Router compromise is such a big issue in itself that further issues are not worth worrying



Our view on Compromised routers

- You should consider threat of compromised routers and their further consequences

Reason – Compromised routers

- Routers can be fully compromised
  - Routers have bugs and there are attacks where routers may be compromised
  - Reported in [Persistent]

Reasons – Why worry about OSPF attacks from a compromised router?

- Is a compromised router's locus of control limited to itself?
- OSPF attacks can be a mechanism to extend the sphere of control of the compromised router
  - e.g., controlling the LSAs of another router

  - OSPF attacks work as a *force-multiplier* to a compromised router

Do you know whether your router(s) are compromised?

- How do you find out?
- Attackers do not want to reveal that a machine is compromised
- Greater threat because of their ability to go undetected
- Have you checked your routers for compromise of late?
- Are the vendors providing mechanisms for this check?

Identifying compromised routers

- How do you come to realize that a router is actually compromised?
- Further consequences may make you aware that a router is compromised
  - e.g., Repeated fight-back attempts may indicate a mis-configured, buggy, or a compromised router in your network

Reasons – Is it an attacker or a bug?

- Compromised router is a good model of
  - Malicious attacker
  - Software bugs
  - Hardware bugs
  - Misconfiguration
- Examples
  - MaxAge
  - [Jinao] reports an insider attacker sending MaxAge maliciously
  - [Draft-dong-ospf-maxage-flush-problem] considers MaxAge issues seen because of hardware or software bugs

Bottom line

OSPF attacks from compromised router are important

Agenda

- Brief Introduction to OSPF
- Attackers, Goals and Consequences
- **Various types of attacks and their mitigation**
  - Remote attacks
  - Compromised router attacks
- Best practices
- Q&A

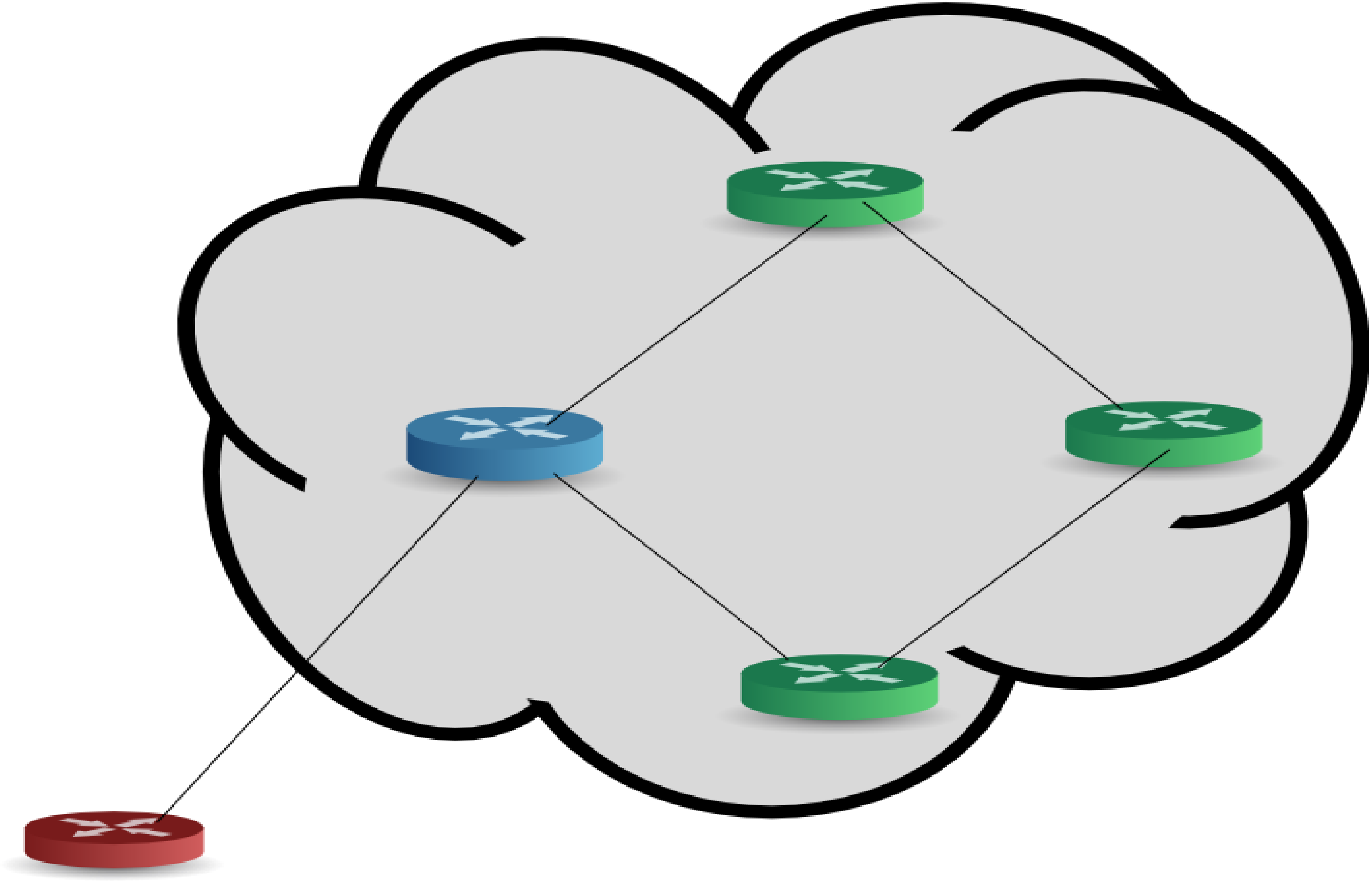
Agenda

- Brief Introduction to OSPF
- Attackers, Goals and Consequences
- **Various types of attacks and their mitigation**
  - **Remote attackers**
  - Compromised router attacks
- Best practices
- Q&A

Remote attackers (Part 1)

- Remote attackers not inside your routing domain launching attacks
- Attacks made possible by misconfiguration

Remote attackers (Part 1)



Remote attackers (Part 1) - Mitigation

- Check for misconfiguration on client facing links
- Use “passive” where required

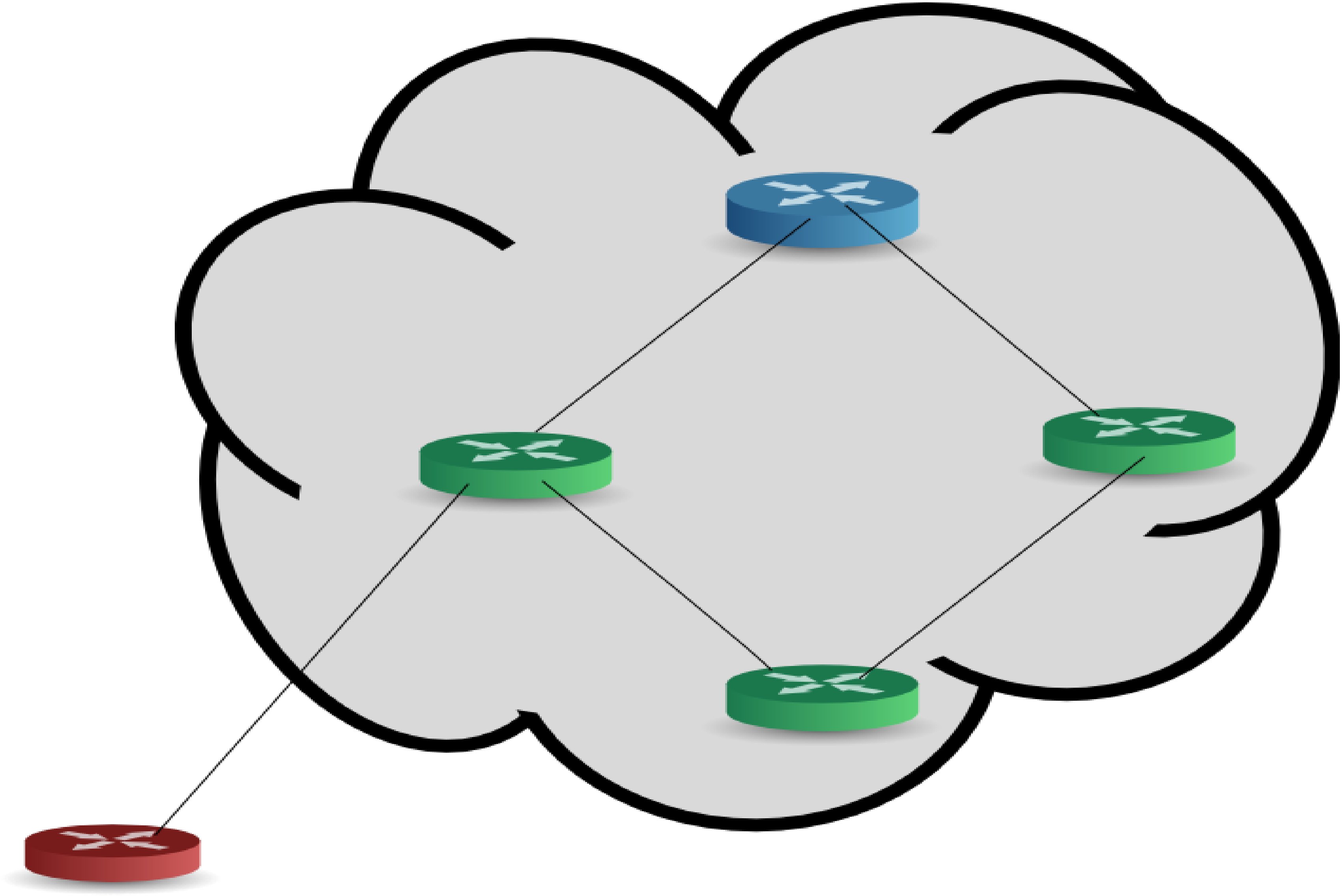
Remote attackers (Part 1)

Demonstration

Remote attackers (Part 2)

- Remote attackers not inside your routing domain launching attacks
- Normally assumes NULL authentication or cracked crypto keys

Remote attackers (Part 2)



Remote attackers (Part 2) - Mitigation

- RPF
  - Reverse path forwarding check for spoofed source IP addresses at boundary of domain
- TTL Security
  - Very powerful and efficient mitigation mechanism

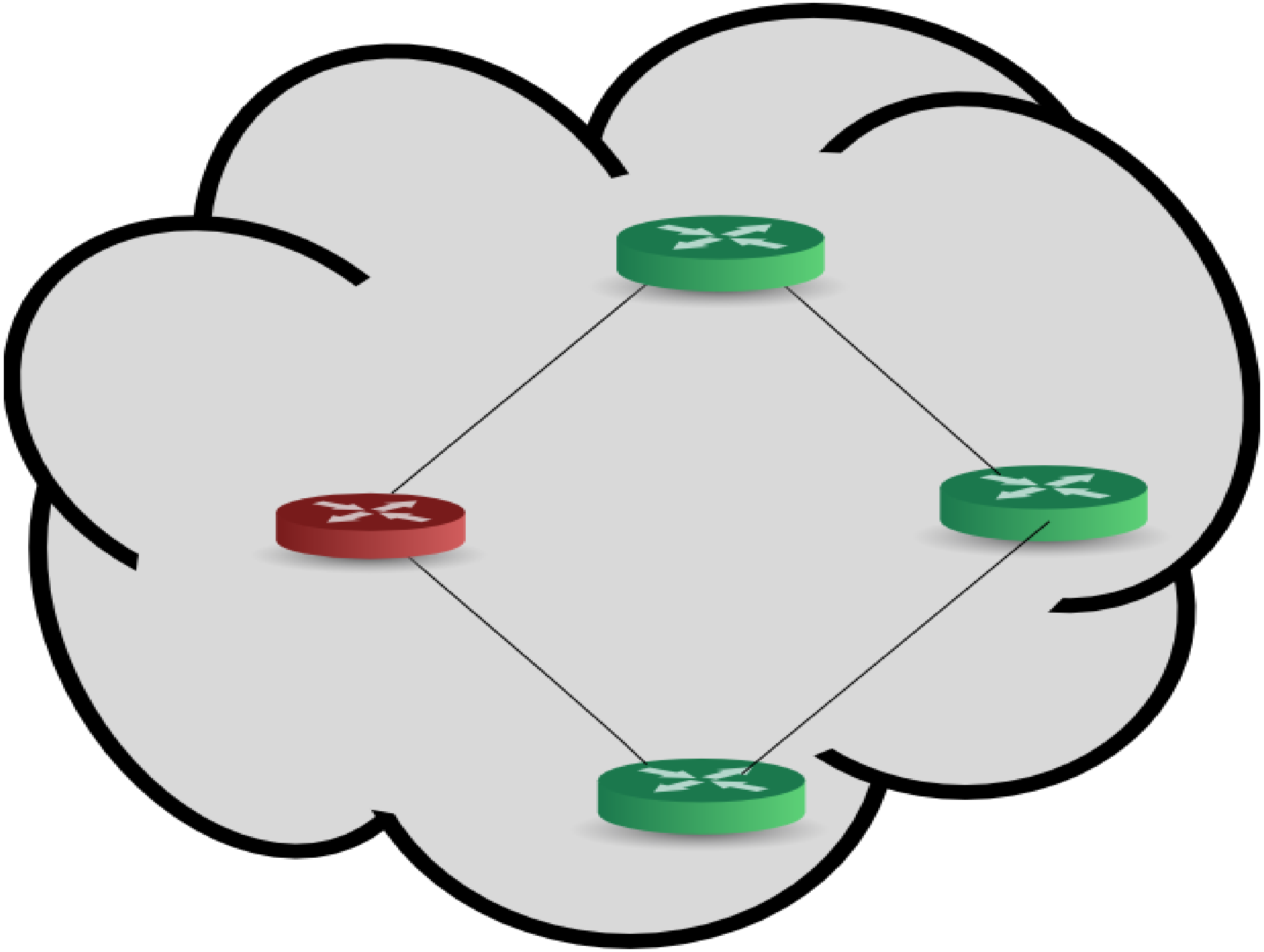
Agenda

- Brief Introduction to OSPF
- Attackers, Goals and Consequences
- **Various types of attacks and their mitigation**
  - Remote attacks
  - **Compromised router attacks**
- Best practices
- Q&A

Compromised Routers

- Send false information in its own LSAs
- Shutdown itself
- Repeatedly issue new LSAs
- Leads to network churn
  - Routing table re-computation
  - Flooding of LSA

Compromised Routers



Mitigations

- Keep a tab on number of SPF runs
  - OspfSpfRuns in OSPF MIB

Compromised router masquerading as ASBR

- Masquerade as an ASBR
- It allows a router to introduce External LSAs in the OSPF domain
- Attacker sends external LSAs making itself the best choice
- Consequences
  - Disrupt traffic destined outside AS
  - Make itself Man-in-the-middle
- Reported in [draft-ietf-rpsec-ospf-vuln-02]

Mitigation

- NMS should check consistency between LSDB and intended configuration of the boxes in the network
- You will notice if an unintended ASBR is in the network

Limitations

Sphere of influence limited

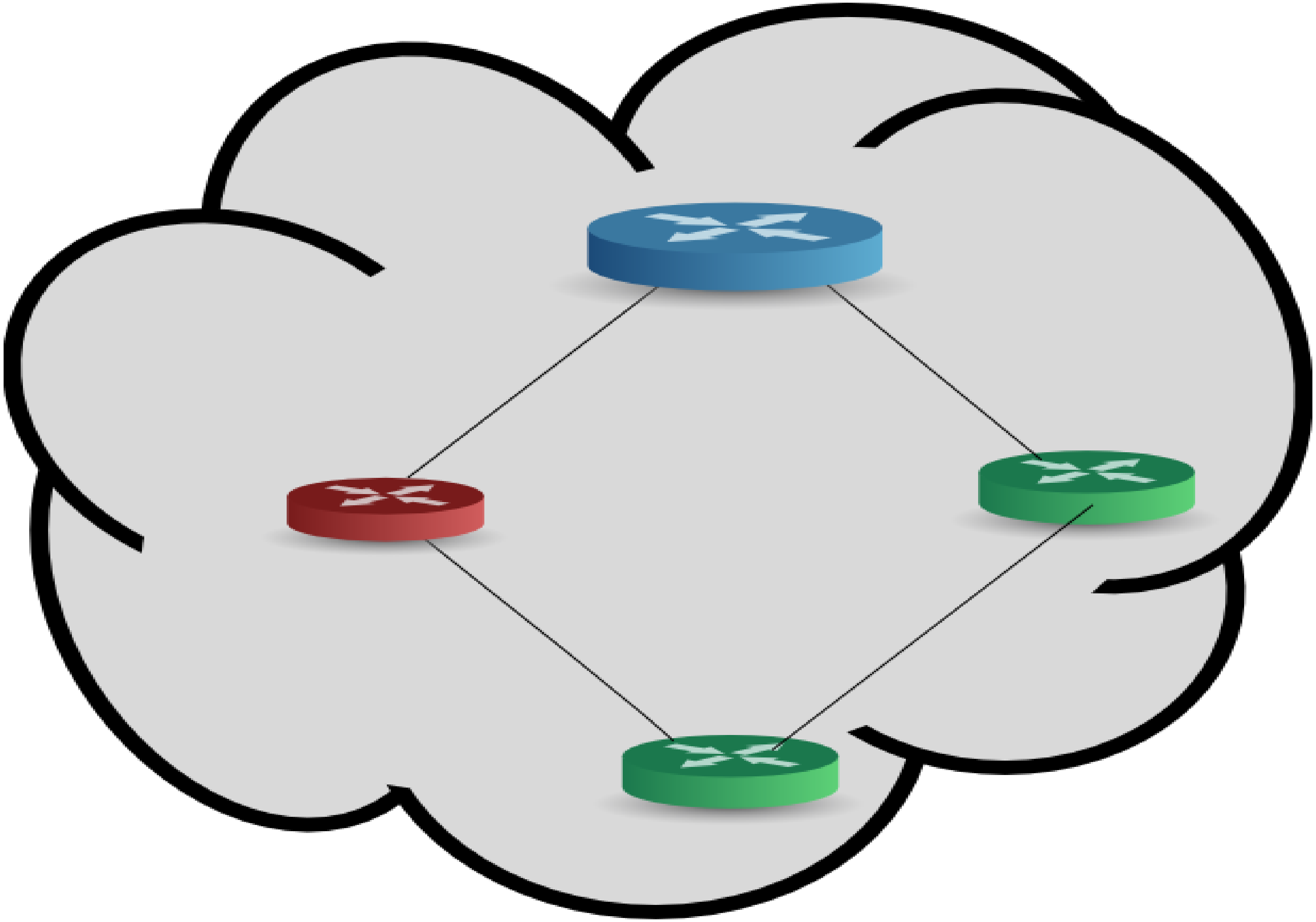
MaxAge LSAs

- A malicious or hardware or software bug modifying LSAs to MaxAge

- Leads to network churn
  - Black-holing of related traffic
  - Routing table re-computation
  - Flooding of LSA

- Reported in [draft-dong-ospf-maxage-flush-problem-statement]

MaxAge LSAs



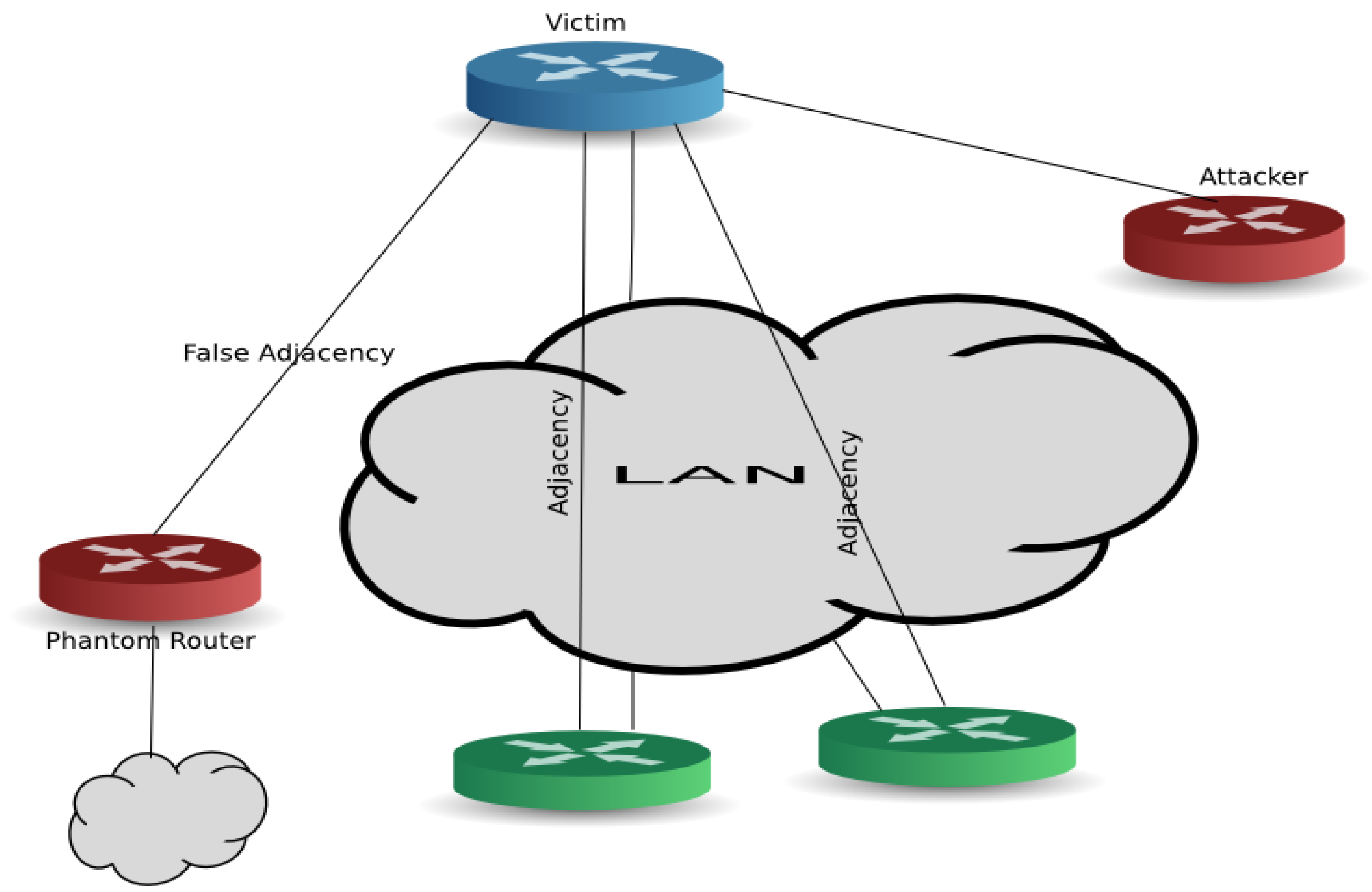
MaxAge LSAs - Mitigation

- If fight-back trap is available, this situation can be detected
- Remedial action can be taken after analyzing the cause

Remote false adjacency

- Assumes compromised router and same keys in the entire network or NULL keys
- Creates phantom router
- Phantom router can advertise LSAs to influence routing table
  - Black-hole traffic etc
- Reported in [Persistent]

Remote false adjacency (contd.)



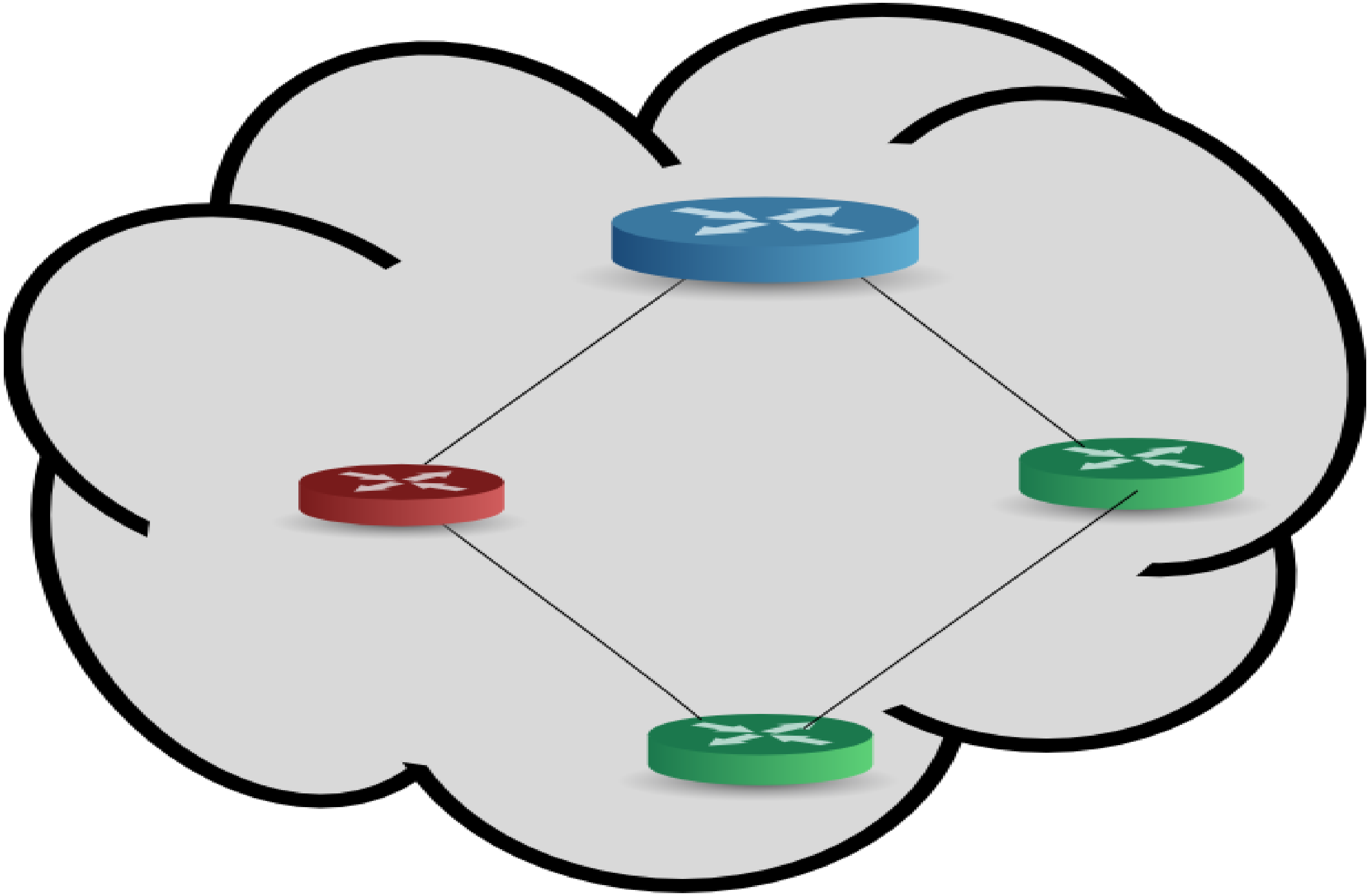
Remote false adjacency - Mitigation

- Diverse keys on different networks
- Enable TTL security

Seq++ attack

- Compromised router sends an LSA for victim with a LS sequence number higher than current sequence number and fake information
- Effects
  - Influences routing tables of other routers because it is a newer LSA
  - Loops, black holing, route the traffic towards itself
- Reported in [JiNao] [draft-ietf-rpsec-ospf-vuln-02]

Seq++ attack



Seq++ attack (contd.)

- OSPF standard
  - “a router will never emit its LSAs faster than once every MinLSInterval (5 seconds)”
- Attacker floods the OSPF domain with malicious LSAs at a rate higher than one every MinLSInterval
  - Permanent changes in the routing domain

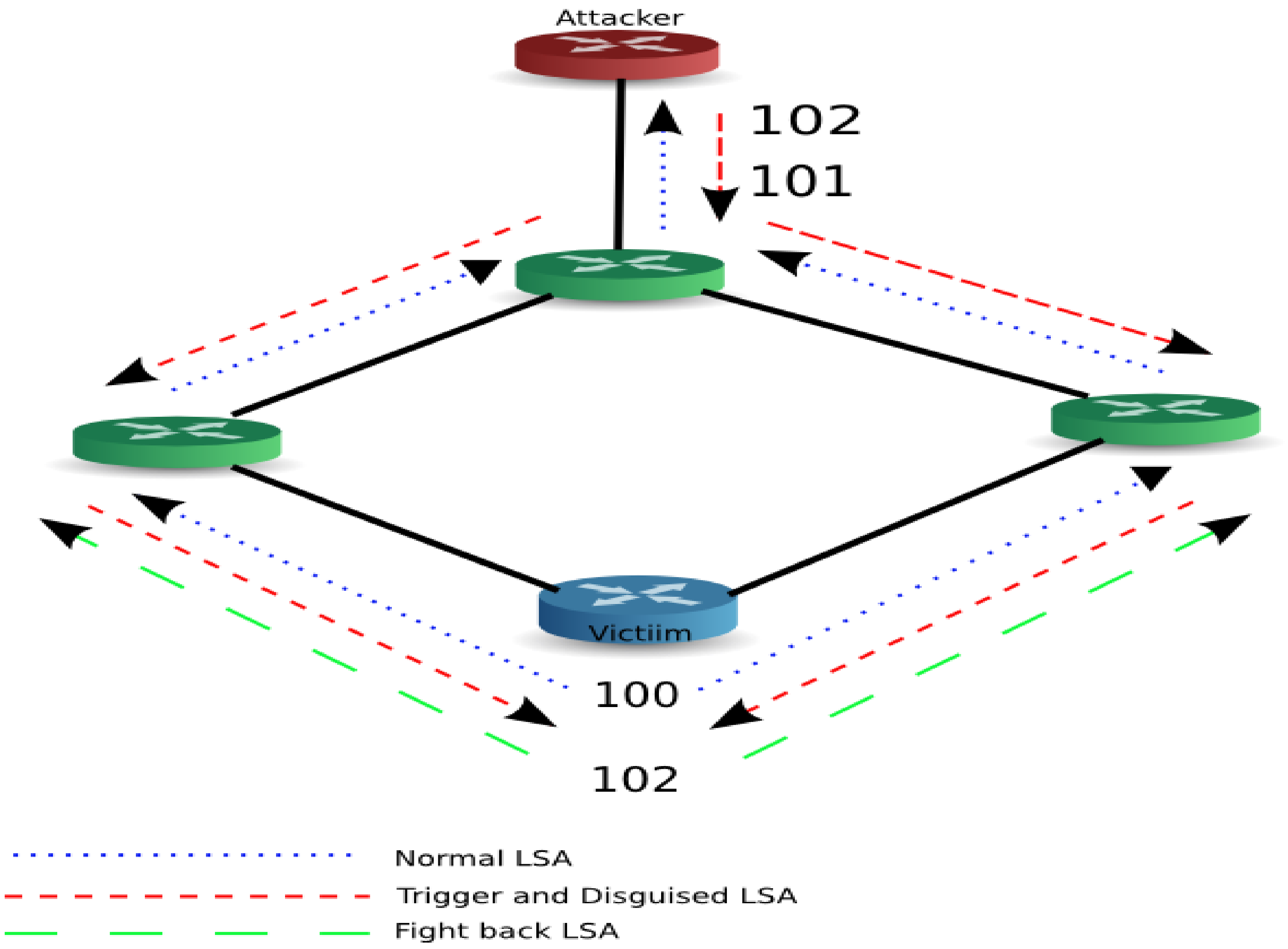
Seq++ attack - Mitigation

- On reception of fake LSA
  - Victim router fights back
- Attacking router needs to repeatedly send newer LSAs
- If fight-back traps are present
  - Large number of traps will be issued
  - Administrator may be alerted about network issue
  - Further action can be taken

Disguised-LSA

- A compromised router sends an LSA for a victim router
- LS Sequence number and checksum are such that fight-back is not triggered
  - Better than previous attack
- Corrupts LS database
  - Influences routing table
- Reported in [Persistent]

Disguised-LSA (contd.)



Disguised-LSA - Mitigation

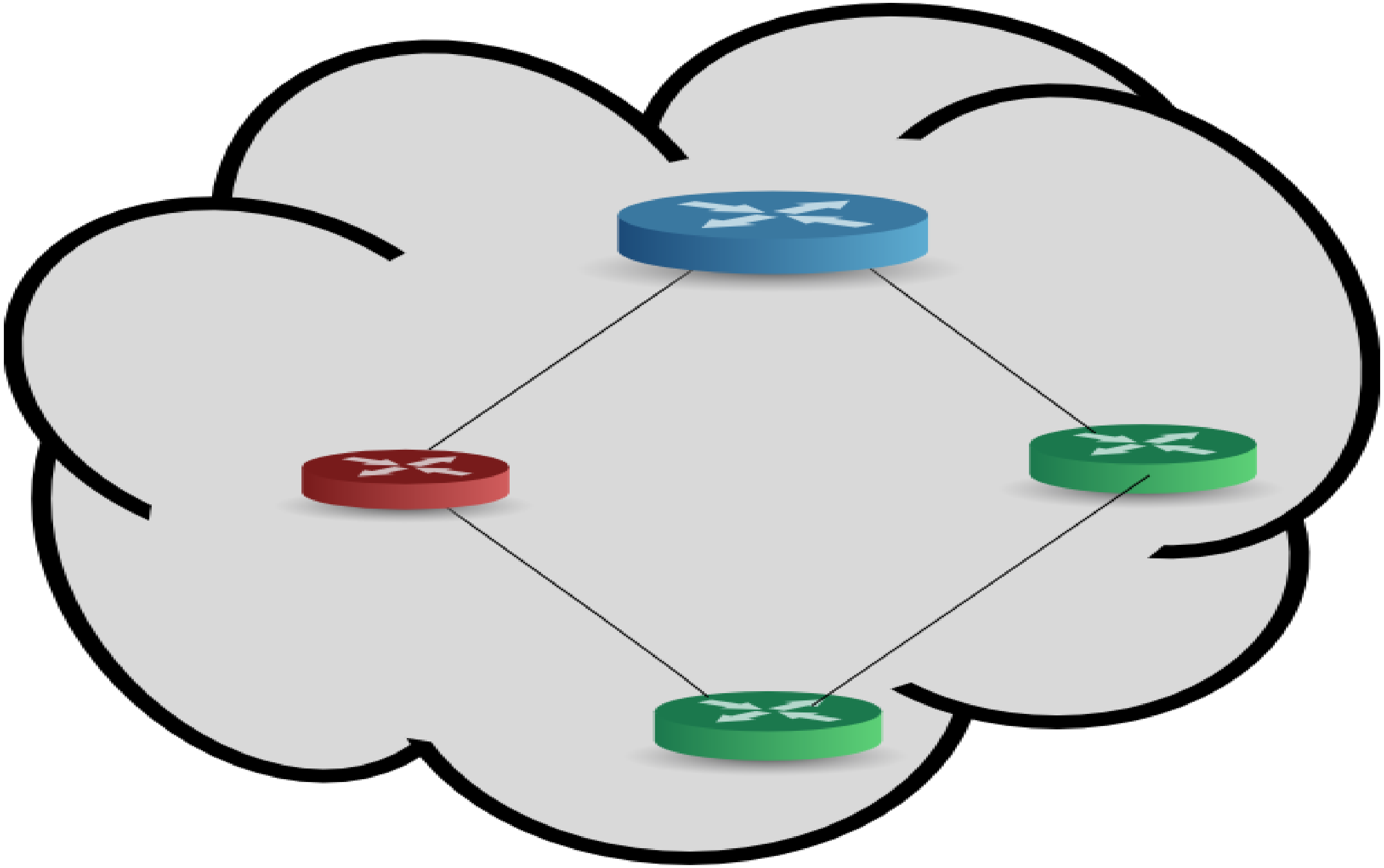
- Detection
  - Fight-back traps will be issued but at a lesser frequency (once half-an-hour)

- Prevention
  - Randomize OSPF LSA sequence numbers
  - Recently proposed draft
    - draft-manjuldtv-ospf-sequence-number

Persistent Poisoning

- A compromised router sends an LSA for a victim router with matching LS ID but not adv. Router ID
- Fight-back not triggered
- Routing table calculation uses the poisoned LSA rather than LSA from victim router
- Vulnerability reported as CVE-2013-0149
- Reported in [PersPoison]

Persistent Poisoning

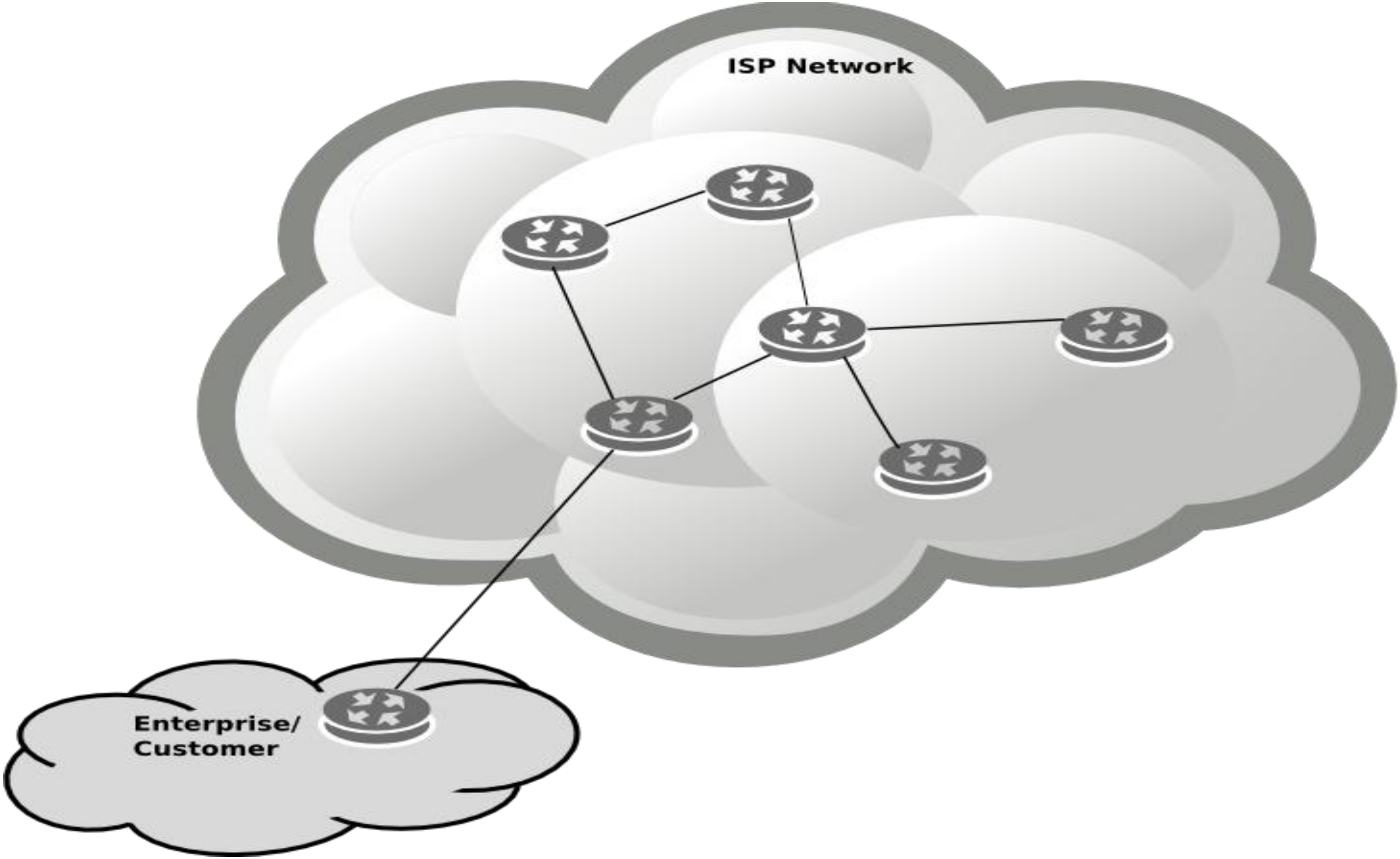


Persistent Poisoning - Mitigation

- OSPF protocol design bug
- Vendor patch required
- Many vendors provided this

Agenda

- Brief Introduction to OSPF
- Attackers, Goals and Consequences
- Various types of attacks and their mitigation
  - Remote attacks
  - Compromised router attacks
- **Best practices**
- Q&A



Reference OSPF Network

Transit-Only Networks

- Based on RFC 6860
- Hides transit-only networks
- Especially useful in preventing remote attackers
- Hides prefixes of transit networks in routing tables

Transit-Only Networks (contd.)

Transit Only Networks can be configured by suppressing the prefixes. Sample configuration are shown below.

Nivetti OS

```
configure> modify parameter-group router traffic
Info: Parameter group instance loaded for modification.
configure> set ipv4 ospf-v2 suppress-prefixes yes
configure> save
```

JunOS

No references available

IOS

```
(config)# router ospf 10
(config-router)#  network 192.16.64.0 0.0.0.255 area 0
(config-router)#  prefix-suppression
```

Unnumbered Interfaces

- If transit-only networks are not possible then unnumbered interfaces may be used
- No host route is generated for these interfaces and no IP packets can be addressed to these interfaces.
- These interfaces are like hidden interfaces.

Unnumbered Interfaces(contd.)

Sample configuration to configure unnumbered interfaces is shown below.

Nivetti OS

```
configure> create parameter-group --force interface e10/0/2
Info: Parameter group instance loaded for modification.
configure> set enable yes
configure> set ip router “traffic”
configure> set ip ipv4 enable yes
configure> set ip ipv4 ospf-v2 enable yes
configure> save
```

JunOS

```
interfaces {
   so-6/1/0 {
       unit 0 {
          family inet;
       }
   }
}
```

IOS

```
(config)# interface Serial 0
(config-if)# ip unnumbered Ethernet 0
```

Crypto Support

- Always enable crypto as it improves security
- Bonus: They help in catching corruption caused by hardware and software bugs
  - Better than existing non-crypto checksum
  - Includes LS Age also in consideration.
  - Same IP Checksum or LSA checksum(Fletchers) is possible but not the crypto checksum.
- Are you using different keys on different LANs?

Crypto Support (contd.)

MD5 crypto support can be enabled using the following sample configuration.

Nivetti OS

```
configure> modify parameter-group interface ge/0/0/1
Info: Parameter group instance loaded for modification.
configure> set ip ipv4 ospf-v2 authentication auth-1
configure> save
configure> create parameter-group ospf-v2-authentication auth-1
configure> set type cryptographic
configure> add key 1
configure> enter key 1
configure> set algorithm keyed-md5
configure> set secret "ab$c1"
configure> save
```

JunOS

```
area 0.0.0.0 {
    interface so-0/2/0.0 {
        authentication {
            md5 5 key "$9$pXXhuIhreWx-wQF9puBEh"; ## SECRET-DATA
        }
    }
}
```

IOS

```
(config)# interface GigabitEthernet0/0
(config-if)#  ip ospf message-digest-key 1 md5 ab$c1          !--- Message digest key with ID "1" and Key value (password) is set as "ab$c1".
(config)# router ospf 10
(config-router)# area 0 authentication message-digest         !--- MD5 authentication is enabled for all interfaces in Area 0.
```

Crypto Support (contd.)

SHA-1 crypto support can be enabled using the following sample configuration.

Nivetti OS

```
configure> modify parameter-group interface ge/0/0/1
Info: Parameter group instance loaded for modification.
configure> set ip ipv4 ospf-v2 authentication auth-2
configure> save
configure> create parameter-group ospf-v2-authentication auth-2
configure> set type cryptographic
configure> add key 1
configure> enter key 1
configure> set algorithm hmac-sha-1
configure> set secret "ab$c1"
configure> save
```

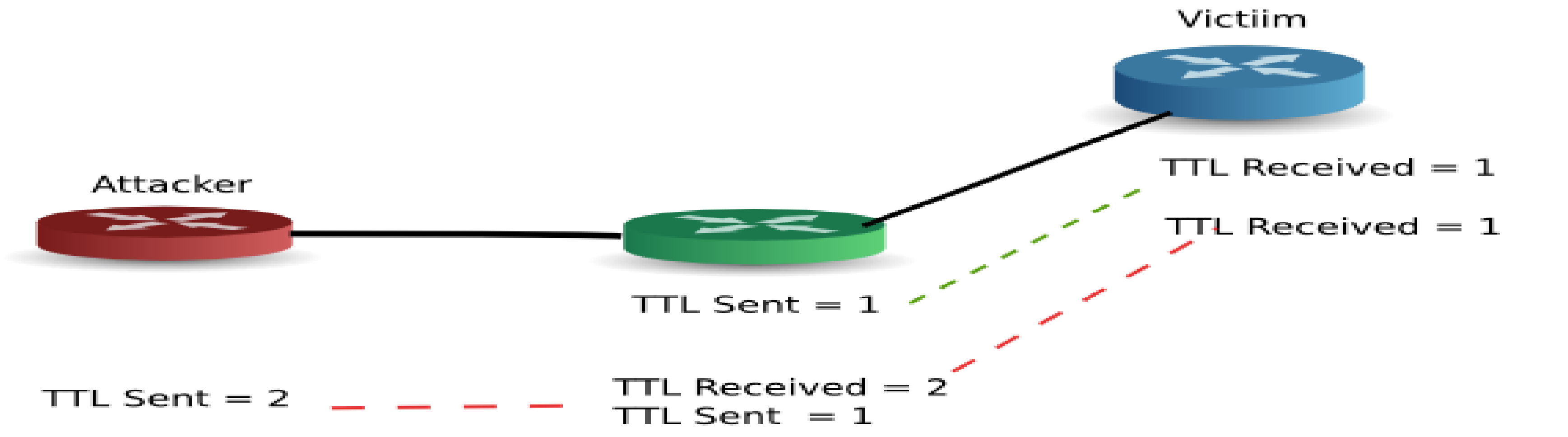
JunOS

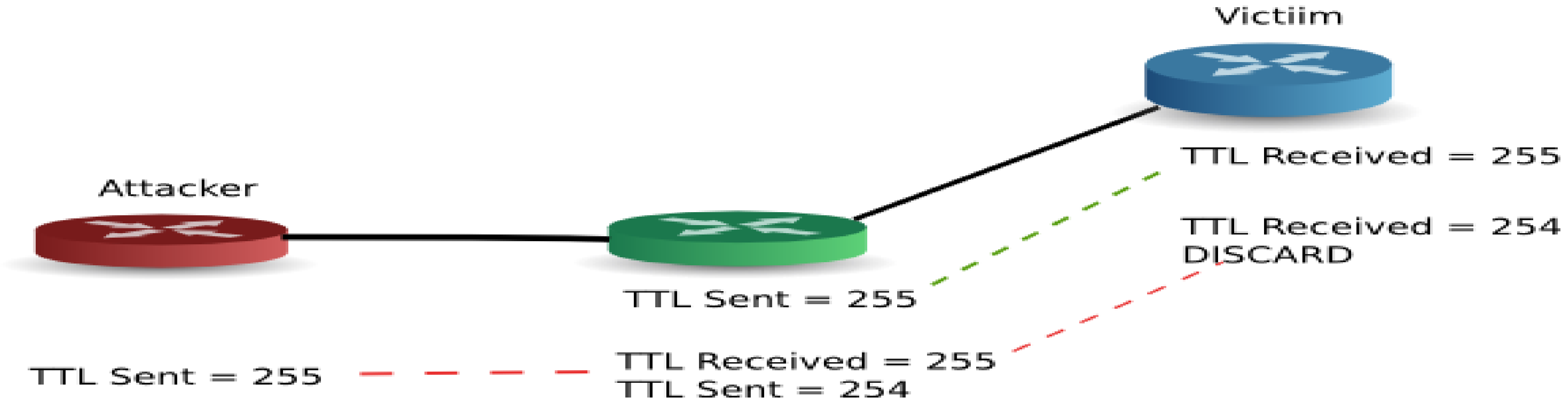
No reference available.

IOS

No reference available.

TTL Security





TTL Security

TTL Security for OSPF protocol can be enabled as shown in below sample configurations.

Nivetti OS

```
configure> modify parameter-group interface if-s4-p1
Info: Parameter group instance loaded for modification.
configure> set ip ipv4 ospfv2 ttl-security enable
configure> save
```

JunOS

No references available

IOS

```
(config)#interface GigabitEthernet0/0
(config-if)#ip ospf ttl-security
```

RPF(Anti-spoofing or Ingress Filtering)

Generally used at network ingress where symmetric routing is used. It can be enabled in various vendor configurations as shown below.

Nivetti OS

- Enabled at the interface level

```
configure> modify parameter-group interface if-s4-p1
Info: Parameter group instance loaded for modification.
configure> set ip ipv4 reverse-path-check enable
```

- Enabled only for ospfv2 on the interface

```
configure> modify parameter-group interface if-s4-p1
Info: Parameter group instance loaded for modification.
configure> set ip ipv4 ospfv2 reverse-path-check enable
```

JunOS

```
interfaces {
    so-0/0/0 {
        unit 0 {
            family inet {
                rpf-check
            }
        }
    }
}
```

IOS

```
(config)#interface GigabitEthernet0/0
(config-if)#ip verify unicast reverse-path
```

Fight back traps/notification

- Mechanism to notify administrator that OSPF is triggering fight backs.
- Frequent notifications point to issues
- Indicates malicious entities
- Router-id misconfiguration
- Indicates partition

Nivetti OS

```
configure> modify parameter-group router global
Info: Parameter group instance loaded for modification.
configure> set ipv4 ospf-v2 security lsa-fightback-notification enable
configure> save
```

LSDB Checksums

Various LSDB 32 bit checksums can be retrieved via SNMP and compared for inconsistencies.

❖**OSPF-MIB:ospfExternLsaCksumSum { ospfGeneralGroup 7 }**
External link state advertisements (LS-type 5)

❖**OSPF-MIB:ospfAsLsaCksumSum { ospfGeneralGroup 25 }**
AS-scope link state database

❖**OSPF-MIB:ospfAreaLsaCksumSum { ospfAreaEntry 8 }**
Link state advertisements in an area. Excludes external (LS type-5) link state advertisements.

These can be retrieved from multiple routers and compared using standard NMS.

OSPF consistency checker tool

- It checks consistency between LSDB as collected from various routers and intended OSPF configuration on the them
- Tool checks
  - Checksum for LSDB synchronization across network via checksum field to see whether network partitioned
  - Is there consistency between configured ASBRs and reporting ASBRs
  - Etc.

- Part of Nivetti OS package. Similar tools might be available for other OEM products.

Randomized Sequence Numbers

As detailed earlier, some attacks use predictable nature

Nivetti OS

```
configure> modify parameter-group router global
Info: Parameter group instance loaded for modification.
configure> set ipv4 ospf-v2 security sequence-number-generation ?

normal : One up sequence number generation mechanism will be used.
random : All sequence number will be randomized in the range configured.
random-fightback : One up sequence number generation mechanism will be used for normal  lsa generation
                   but it will be randomized in the configured range for fightback lsa generation.
```

Others

- Mono-culture is dangerous both in agriculture and networks. Have vendor and software diversity.
- NMS should run OSPF consistency checking tool periodically. Use consistency checker tool periodically.
- RFC 7474 crypto support. Demand support for this as this avoids crypto replay attacks.
- Enable syslogs for database overflow
- Vendor plugs the vulnerabilities as and when they are reported. Upgrade to newer releases as early as feasible.

References

- RFC 6860 – Hiding Transit only networks in OSPF
- [Jinao] “Wu et al, JiNao: Design and implementation of a scalable intrusion detection system for the OSPF routing protocol, Journal of computer networks and ISDN systems”
- [Persistent] “Nakibly et al, Persistent OSPF Attacks, NDS 2012”
- [PersPoison] “Nakibly et al, OSPF vulnerability to persistent poisoning attacks: a systematic analysis, CSAC 2014”

References

- [Partition] “Cohen et al, Small lies, lots of damage: a partition attack on link-state routing protocols, CNS 2015”
- [draft-ietf-rpsec-ospf-vuln-02] “Jones et al, OSPF security vulnerability analysis, Internet draft”
- [Draft-dong-ospf-maxage-flush-problem] “Dong et al, OSPF corrupted Maxage LSA flushing problem statement, Internet draft, 2016”
- [draft-jakma-ospf-integrity-00] “Jakma et al, Stronger, automatic integrity checks for OSPF packets, Internet draft”
- [draft-manjuldtv-ospf-sequence-number] “Manjul et al, OSPF LSA sequence number generation, 2016”

Questions?