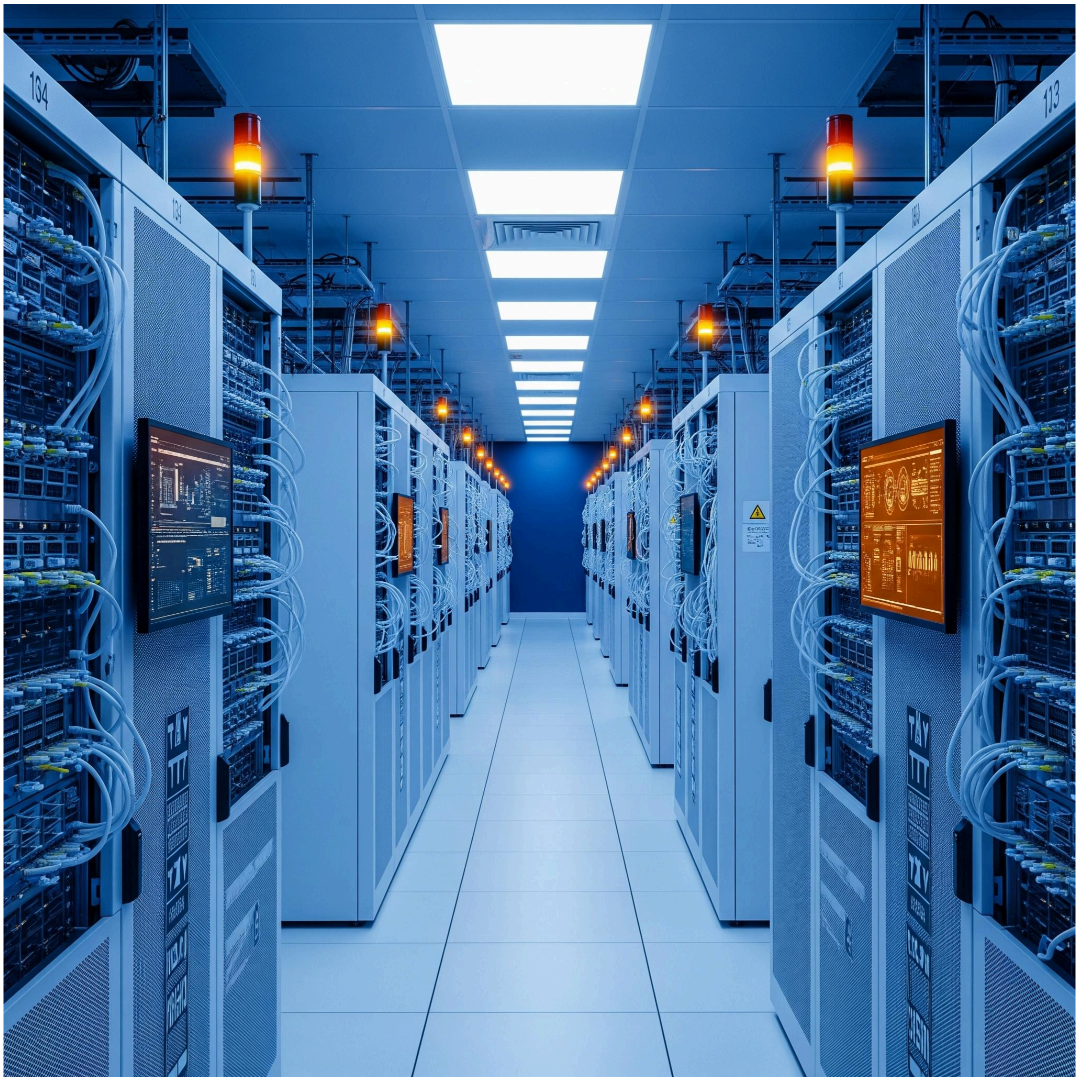


OSPF and MPLS LDP Best Practices for Service Providers

Pablo Díaz - Senior Network Engineer
linkedin.com/in/pdiazd
contact@pdiazd.com
August 2025

Content

1 Introduction

1.1 Overview

This document is intended to provide the best practices for OSPF and MPLS on Service Provider networks. We are also going to analyze different forms or points to improve its network parameters.

1.2 Document Scope

This document is intended to provide the best practices for IGP and LDP. We are also going to analyze and recommend different forms of improving its network. This document includes:

- Details of the features and technologies to be used
- General configuration templates

1.3 Audience

This document is directed to Network Engineering and Operations teams.

2 Protocol Optimization Best Practices

This section is to provide the best practices of the technologies and features to be used in the MPLS network.

2.1 OSPF

OSPF is a “Link-State” protocol that uses the concept of areas to provide hierarchy within the same administrative system. All the devices that belong to the OSPF process know all the OSPF topology information associated with the area, and use the Dijkstra algorithm to select a loopless path with the lowest cost for each router in the area.

2.1.1 OSPF Process

The OSPF process will be configured on new devices in the same way as in the ones currently operating in order to keep the configuration standardized. Area 0 will be used for the links to other devices and the loopback interfaces should be passive in the process.

OSPF Process configuration – IOS / IOS-XE

```
!
router ospf 1
 network <address> <wildcard-mask> area 0
 passive-interface Loopback 0
 log-adjacency-changes
!
```

OSPF Process configuration – IOS-XR

```
!
router ospf 1
 log adjacency changes detail
 area 0
  interface Loopback0
   passive enable
  interface <interface-id>
  !
 !
!
```

The loopback interfaces of the devices should be /32, generated by the node as internal to the area (without the redistribute command) and should be passive at the OSPF level.

The “log-adjacency-changes” command is recommended as a best-practice to have as a useful tool during troubleshooting.

2.1.2 Router identifier in OSPF

Each router in the ISP network needs a router-id that identifies it in the OSPF database. This router ID can be any number, not necessarily of an active interface of the router itself, and works as a reference in the topology database to identify which was the router that originated the LSA. By default, the IOS takes the interface with the highest IP address. In case that the device has Loopback interfaces configured, the IOS prefers them and in case that there is more than one, the tie breaker is the highest IP address.

Router-id configuration – IOS / IOS-XE / IOS-XR

```
!
router ospf 1
 router-id <address Loopback 0>
!
```

Reference Bandwidth

For all the links higher than 100Mbps it is advisable to change the defaults for the link cost, since otherwise the cost calculated would be less than 1.

In today’s networks, most of the links within the OSPF network are 1/10/100GigabitEthernet, so it is recommended to use the reference value 1.000.000.

Reference BW configuration – IOS / IOS-XE / IOS-XR

```
!
router ospf 1
 auto-cost reference-bandwidth 1000000
!
```

2.1.3 Type of OSPF Network

An Ethernet interface is broadcast by default in IOS. If we consider that all the Core interfaces are point-to-point, the fact that they are configured as broadcast when selecting a DR and a BDR generates a higher load of information in the devices, as well as an increase of time on failure detection. It is recommended then that all the interfaces are configured as point-to-point, so the time needed to establish an adjacency is reduced considerably, and there are less Type 2 LSAs in the network.

OSPF Network type configuration – IOS / IOS-XE

```
!
interface <interface-id>
 ip ospf network point-to-point
!
```

OSPF Network type configuration – IOS-XR

```
!
router ospf 1
 area 0
  interface <interface-id>
   network point-to-point
  !
 !
!
```

2.1.4 Improvements to SPF

It is recommended to consider using new timers for SFP and LSA different from the ones currently in production. This implies the configuration of: event or failure detection timer, update interval or change spreading, timer to begin the SPF computing, timer for the SPF algorithm to start running, timer for the routing table update interval, update of the RIB/FIB (CEF) table.

Configuration of SPF improvements configuration – IOS / IOS-XE

```
!
router ospf 1
 timers throttle spf 50 50 5000
 timers throttle lsa all 0 20 5000
 timers lsa arrival 15
 timers pacing flood 15
!
```

Configuration of SPF improvements configuration – IOS-XR

```
!
router ospf 1
 timers throttle spf 50 50 5000
 timers throttle lsa all 0 20 5000
 timers lsa min-arrival 15
 timers pacing flood 15
!
```

2.1.5 Authentication in OSPF

OSPF has a hashing system implemented in order to authenticate the neighborhood sessions between the devices of the same administrative system. It is recommended to use the global type of authentication.

Authentication configuration in OSPF – IOS / IOS-XE

```
!
interface <interface-id>
 ip ospf message-digest-key 1 md5 <password>
!
router ospf 1
 area 0 authentication message-digest
!
```

Table 10: Authentication configuration in OSPF – IOS-XR

```
!
router ospf 1
 area 0
  authentication message-digest
  message-digest-key 1 md5 <password>
 !
!
```

2.1.6 LSA Max-metric on Startup

When a router is restarted, it will try to become part of the network IP path as soon as OSPF neighborships get established, producing suboptimal routing and/or blackholes while the router is not completely initialized. To prevent the router to be a valid path until it is completely initialized, it is necessary to raise the advertised cost of their interfaces until all OSPF neighborships are in READY state by modifying the Router LSA information that is going to be sent while the router is booting up.

LSA Max-metric on startup configuration on OSPF – IOS / IOS-XE / IOS-XR

```
!
router ospf 1
 max-metric router-lsa on-startup 600
!
```

2.1.7 OSPF Flood Reduction

By design, OSPF requires link-state advertisements (LSAs) to be refreshed as they expire after 3600 sec. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 min to around 50 min or so. This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires.

The OSPF Flooding Reduction feature works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set, thus making them DoNotAge (DNA) LSAs.

OSPF Flood Reduction configuration on OSPF – IOS / IOS-XE

```
!
interface <interface-id>
 ip ospf flood-reduction
!
```

Table 13: LSA Max-metric on startup configuration on OSPF – IOS-XR

```
router ospf 1
 flood-reduction
!
```

2.1.8 Recommendations for OSPF

In order to apply the best practices recommendations, it's necessary to mention the following:

1. Inside the OSPF process ID in OSPF it is necessary to specify a router ID as a best practice, and to know what is the specific neighbor, which a router has a session with.
2. It’s recommend to enable a reference bandwidth with a value of 100000 (100Gbps) to have congruency with the link capacities (TenGigabitEthernet or GigabitEthernet), so in case of having a 10G connection the cost will be 10 and for 1G connection will be 100, and the TenGigabitEthernet link will be preferred to send all the traffic.
3. In order to have a most stable, reduced and efficient routing table Cisco recommends suppressing the LSA type 2 between routers connections. By default, the network type in the Ethernet interfaces is broadcast, and to suppress LSA type 2 is recommended to define Ethernet links as “ip ospf network point-to-point”.

4. It is recommended a tuning in the LSA and SPF timer with the simple reason to speed the convergence when a link failure occurs and to control LSA flooding in case of link inestabilities.
5. For security reasons it is necessary to enable MD5 between OSPF neighbors in order to exchange routing update information in a secure manner and avoid undesired devices to be part of the MPLS network.

2.2 LDP

LDP is responsible for distributing the labels associated with all the destination IP prefixes in an MPLS network. The labels will be assigned to every address in the global routing table. This global routing table is created and maintained by the IGP which in this case is OSPF. Every destination IP prefix will be a loopback or a network interface address and normally there should not be any customer IP address in the global routing table.

It is recommended to enable LDP. The main reason to do this is to avoid having the BGP process in the MPLS core devices, which should keep the number of processes to a minimum to accomplish their role properly, as well as to allow the MP-BGP feature to be enabled.

2.2.1 MPLS Label Protocol LDP

To specify the default label distribution protocol for a platform, it’s necessary to use the “mpls label protocol ldp” command. LDP is the label exchange protocol for MPLS which provides the means for LSRs to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information. LDP can be enabled both in the global system and, as per interface label exchange protocol.

Basic LDP configuration - IOS / IOS-XE

```
!
mpls label protocol ldp
!
```

Basic LDP configuration - IOS-XR

```
!
mpls ldp
!
```

2.2.2 MPLS Label Protocol LDP

MPLS LDP has the possibility to be enabled in a per interface basis and to all of the OSPF enabled interfaces automatically.

Enabling it on a per interface basis allows the operators to control the LDP adjacencies to be formed in a deterministic manner and, also, to protect the LDP topology of unwanted adjacencies that could introduce blackholes or suboptimal MPLS forwarding.

Enabling LDP per Interface configuration - IOS / IOS-XE

```
!
interface <interface-id>
 mpls ip
!
```

Basic LDP per Interface configuration - IOS-XR

```
!
mpls ldp
 interface <interface-id>
!
```

2.2.3 Router-id in LDP

Each router with LDP must have a unique identifier in the network to distinguish it from others when establishing TCP sessions with other devices. This router-id can take any numeric value in the format of an IP address, which doesn't need to be present in the configuration.

If it is not configured manually, by default the router takes the highest logical interface IP address, in case there are no logical interfaces router takes the highest IP address of their active interfaces.

Router-id configuration in LDP – IOS / IOS-XE

```
!
mpls ldp router-id loopback0 force
!
```

Router-id configuration in LDP – IOS-XR

```
!
mpls ldp
 router-id <loopback0 IP>
!
```

2.2.4 LDP Monitoring

In IOS-XR MPLS LDP doesn’t send explicit notification messages to the router log by default, unless it is configured. It is recommended to notify the router about the LDP adjacency changes.

LDP monitoring configuration – IOS-XR

```
!
mpls ldp
 log
  adjacency
  nsr
  graceful-restart
 !
!
```

2.2.5 LDP Session Protection

LDP provides two mechanisms for potential LDP peer discovery and protection: LDP Basic Discovery and LDP Extended Discovery.

LDP Basic Discovery supports the discovery of directly connected neighbors at a link level (by UDP 646 destination 224.0.0.2), so it is also known as Link Discovery while LDP Extended Discovery supports the discovery of neighbors that are not directly connected at a link level.

LDP Basic Discovery uses UDP Link Hellos and LDP Extended Discovery uses LDP Targeted Hellos, in both cases using UDP packets on port 646.

LDP convergence when a link is recovered after it went down can be improved by using LDP Extended Discovery with the neighboring link. If there is an alternate path to the neighbor, and there is a LDP adjacency with Targeted Hello, Extended Discovery makes it unnecessary to establish the LDP session with the neighbor link and re-learn the association of labels when the link is recovered.

When the link goes down, if the peer is reachable by IP, the LDP session is supported and maintained by Extended Discovery, allowing keeping the existing label association. Then when the link comes back up, and the IGP starts using it, the IP address of the neighbor’s link is the only neighbor information required for the LDP convergence.

MPLS LDP Session Protection configuration – IOS / IOS-XE

```
!
mpls ldp session protection
!
```

MPLS LDP Session Protection configuration – IOS-XR

```
!
mpls ldp
 session protection
!
```

2.2.6 LDP and IGP Synchronization

LDP and IGP synchronization guarantees that LDP is fully established before the IGP path is used. Packet loss can occur if LDP and IGP are not synchronized in the following situations:

- When an IGP adjacency is established, the router begins to send packets using this new adjacency before the LDP label interchange has finished between the peers of that link.
- When a LDP session is closed, the router continues sending traffic using the link associated with the LDP peer instead of using an alternate path with a fully synchronized LDP session.

This LDP and IGP synchronization feature:

- Synchronizes LDP and IGP minimizing the packet loss in the above mentioned situations.
- Enables the LDP and IGP synchronization globally on each interface associated with the IGP, in this case OSPF.
- Provides the option to disable the LDP and IGP synchronization on interfaces that don’t require it.

LDP and IGP synchronization configuration – IOS / IOS-XE / IOS-XR

```
!
router ospf {pid}
 mpls ldp sync
!
```

2.2.7 MPLS LDP Advertise - Labels

By default, labels for all destinations are announced to all LDP or TDP neighbors. When it is necessary to keep the control of label distribution between LSRs in MPLS, it’s possible to selectively advertise some labels to LDP neighbors. To control the distribution of locally assigned the mpls ldp advertise – labels command and its variants could be configured. Keep in mind this command should be carefully configured because it can cause loss of services in case any IP prefix is missed.

MPLS LDP Advertise Labels configuration - IOS / IOS-XE

```
!
mpls ldp advertise-label
!
```

After allowing mpls ldp label propagation, the range or label space can be allocated too.

MPLS LDP Label Allocation (Label space) configuration - IOS / IOS-XE

```
!
mpls ldp label
 allocate global host-routes
!
```

MPLS LDP Advertise and Allocation Labels configuration - IOS-XR

```
!
mpls ldp
 address-family ipv4
  label
   local
    allocate for host-routes
   !
  !
 !
!
```

2.2.8 TTL Propagation

The TTL (Time To Live) functionality in MPLS is equivalent to that of traditional IP forwarding. When an IP packet is labeled, TTL value from the IP header is copied into TTL field in the MPLS Label which is called TTL propagation and it helps to avoid loops.

TTL propagation can be disabled to hide the core infrastructure from end users. When TTL propagation is disabled in MPLS, routers set to 255 the TTL value in the MPLS label.

TTL can be disabled for forwarding traffic only, which allows network administrators to use traceroute from routers to troubleshoot problems in the network.

MPLS TTL Propagation configuration - IOS / IOS-XE

```
!
no mpls ip propagate-ttl forwarded
!
```

MPLS TTL Propagation configuration - IOS-XR

```
!
mpls ip-ttl-propagate disable
!
```

2.2.9 Recommendations for LDP

In order to apply the best practices recommendations for LDP, it's necessary to mention the following:

1. Choose label exchange protocol. By default Cisco works with LDP, but it’s very important to set the protocol that will be used for label exchanging, because if someone enables TDP in one router and TDP in the neighbor, then LDP session will not come up.
2. It is recommended to enable MPLS LDP on a per interface basis to avoid setting unwanted LDP neighbors.
3. It’s a recommended best practice setting the LDP router-id which should be a logical interface that gives stability to the network. If any physical interface is chosen as a router–id, whenever the physical interface gets flapping then the MPLS session will flap.
4. When LDP is working with mpls ldp discovery, it is recommended enabling LDP session protection too, reestablishing mpls ldp session with an IP reachable neighbor after a link failure.

5. It is important enabling LDP and IGP synchronization to guarantee that LDP is fully established before the IGP path is used. If synchronization is not enabled and one link gets constantly flapping, mpls ldp session will flap and all traffic will be lost.
6. To protect the MPLS core is necessary to disable propagation of TTL which hides the core to the customers. It is recommended to apply the “no mpls ip propagate-ttl forward” in PE routers.

3 High Availability

Considering that the network belongs to a Service Provider, it is imperative to deploy a high level of redundancy and availability at all network levels. In this section there will be a discussion of High Availability at the following levels:

1. At a device level, hardware related features that provide high availability.
2. At link level, high availability features to be implemented in the links.
3. At service level, high availability features for mobile services.

3.1 At a Device Level

The features at a device level help to prevent the disruption in the forwarding plane when there is a failure in the control plane caused by the switchover of the active Route Processor. The available features are:

- Stateful switchover (SSO)
- Non stop forwarding (NSF) / Graceful Restart
- Non stop routing (NSR)

3.1.1 Stateful Switchover (SSO)

SSO allows line cards, protocols and state synchronization between the active Route Processor and the Standby. With SSO the Standby RP is totally initialized and ready to take control in case that the active RP fails, minimizing the traffic loss due to the switchover. This operating state is called “Hot Standby”.

The different applications being executed in the RP must be supported by SSO to be incorporated to this synchronization mode, which is known as “SSO-aware”. The state information of these applications or protocols is synchronized from the active RP to the Standby.

The SSO-aware implementations are either independent to the HW platform or dependent, as the driver states in the linecards. SSO is the operation mode by default in IOS-XR.

Stateful Switchover (SSO) configuration – IOS

```
!
redundancy
 mode sso
 main-cpu
```

```
  auto-sync running-config
  auto-sync standard
!
```

Stateful Switchover (SSO) configuration – IOS XE

```
!
redundancy
 mode sso
!
```

3.1.2 Non Stop Forwarding (NSF) / Graceful Restart

It refers to the router's ability to keep the forwarding path intact (FIB/CEF) as the control plane restarts after a switchover in the active RP. This implies not only that the device suffering the switchover maintains the packet forwarding, but also that the rest of the neighbor nodes consider it as a valid next-hop. For this, both nodes must agree on this condition by a Graceful Restart.

Through a Graceful Restart, the router initiating the switchover (called NSF Capable) warns its neighbors over each NSF-aware control protocol that it is starting a switchover. If the neighbor is NSF aware, then by a Graceful Restart it starts the control plane reconstruction keeping the forwarding to the commuting node of RP.

As it is required that the forwarding tables are synchronized between the active and standby RP, Cisco NSF always operates along with SSO.

NSF is a feature that is negotiated inside each protocol. Given this fact, if one of the neighbors doesn't have the NSF capability, it will be automatically disabled for this adjacency/neighbor.

It is worthy to mention that the NSF concept has been extended in a way that for some control protocols, SSO stores the operating state completely in the control plane, so it is not necessary to perform the signaling for Graceful Restart. This implementation is called Non-Stop-Routing (NSR) and is a complement of NSF.

3.1.3 Non Stop Routing (NSR)

In case there is an RP failover, NSR is achieved for TCP as well as for the applications (OSPF or LDP). NSR is a high availability method for the routing protocols. The TCP connections and the routing protocols sessions are migrated from the active RP to the standby after the RP failover without the peers even noticing it. What happens really is that the protocols that are running in the standby reestablish the sessions after the standby RP becomes active.

It is an advantage of NSR to not require the help from neighbors. NSR is used for OSPF and LDP in the following cases:

- Route Processor (RP) or Distributed Route Processor (DRP) failover.
- OSPF, LDP or TCP process restart.
- Minimum Disruption Restart (MDR).

3.1.4 OSFP NSF

When an NSF-capable router with OSPF performs a switchover, it must do two tasks to be able to synchronize its Link State Database (LSD) with its OSPF neighbors. First, it has to re-learn the available OSPF neighbors in the network without causing a neighbors reset. Second, it should re-add the LSD contents through the network.

As soon as possible after a switchover, the NSF-capable router sends an OSPF NSF signal to the NSF-aware devices. These devices recognize this as a signal that the relationship with this neighbor must be reset. As the NSF-capable router receives signals from other routers, it can begin building its neighbors list.

Once the relationships with the neighbors are reestablished, the NSF-capable router begins the re-synchronization of its database with all its NSF-aware neighbors. At this point, the routing information is interchanged between the OSPF neighbors. After the interchange is complete, the NSF-capable device uses the routing information to remove the stale routes, and update the RIB and FIB with the new forwarding information. This way, OSPF has completely converged.

OSPF NSF requires that all neighbors are NSF-aware. If the NSF-capable router discovers that there is a non-NSF-aware neighbor in a particular segment, it will disable the NSF capabilities for that segment.

It is recommended to implement OSPF NSF IETF.

OSPF NSF configuration – IOS / IOS-XE / IOS-XR

```
!
router ospf 1
 nsf ietf
!
```

3.1.5 OSPF NSR

OSPF NSR is disabled by default. When NSR is enabled, the OSPF processes in the active RP synchronize all the necessary information with the OSPF processes of the standby RP. When the switchover occurs, the OSPF processes of the new active RP have all the information to continue running and it doesn’t need any help from its peers.

OSPF NSR configuration – IOS / IOS-XE / IOS-XR

```
!
router ospf 1
 nsr
!
```

3.1.6 LDP NSF

MPLS LDP GR works in strict helper mode, which means it helps a neighboring route processor that has MPLS LDP SSO/NSF to recover from disruption in service without losing its MPLS forwarding state. The disruption in service could be the result of a TCP or UDP event or the stateful switchover of a route processor. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding states are recovered.

LDP NSF configuration – IOS / IOS-XE

```
!
mpls ldp graceful-restart timers forwarding-holding 120
mpls ldp graceful-restart
!
```

LDP NSF configuration – IOS-XR

```
!
mpls ldp
 graceful-restart
 graceful-restart reconnect-timeout 120
 graceful-restart forwarding-state-holdtime 120
!
```

3.1.7 LDP NSR

The NSR LDP Support feature allows the Label Distribution Protocol (LDP) to continue to operate across a node failure without losing peer sessions. Before the introduction of nonstop routing (NSR), LDP sessions with peers reset if a Route Processor (RP) failover or a Cisco In-Service Software Upgrade (ISSU) occurred. When peers reset, traffic is lost while the session is down. Protocol reconvergence occurs after the session is reestablished.

When NSR is enabled, RP failover and Cisco ISSU events are not visible to the peer device, and the LDP sessions that were established prior to failover do not flap. The protocol state learned from the peers persists across an RP failover or Cisco ISSU event and does not need to be relearned.

LDP NSR configuration – IOS / IOS-XE

```
!
mpls ldp nsr
!
```

LDP NSR configuration – IOS-XR

```
!
mpls ldp
 nsr
!
```

3.2 At a Link Level

3.2.1 Bi-directional Forwarding Detection (BFD)

Bi-Directional Forwarding (BFD) is a protocol designed to provide a rapid detection in the path of two adjacent devices.

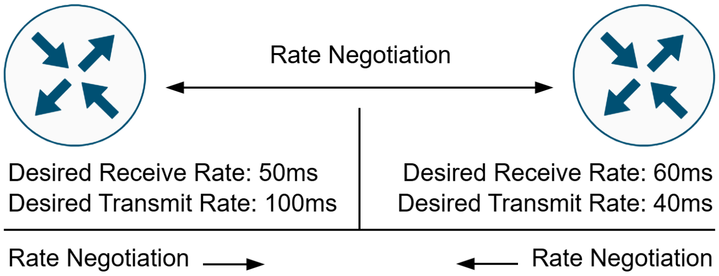
BFD is a unique mechanism that can be used for failure detection over any carrier (POS, GE, etc.) and any protocol level, with a configuration range of detection and overhead times.

The rapid failure detection provides an immediate response in case there is a link or node failure event. BFD has the advantage of detecting the forwarding plane failures that might not be seen in the control plane.

The BFD packets use UDP with destination port 3784 and source ports 49252 and 65535, and since it is designed as a rapid response protocol, BFD control packets generated locally bypass the outbound functionalities of the router.

The main function of BFD is detecting that the forwarding plane is operational.

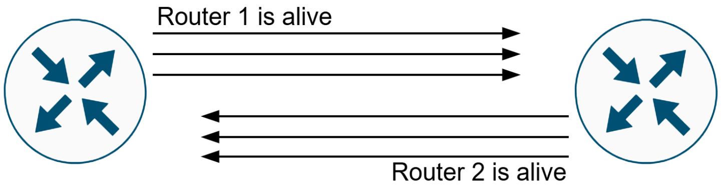
BFD uses two timers that are negotiated in the adjacent nodes, a transmission timer and a reception timer; the system that reports the lowest times is used to determine the transmission ratio.


Rate Negotiation
Desired Receive Rate: 50ms
Desired Transmit Rate: 100ms
Desired Receive Rate: 60ms
Desired Transmit Rate: 40ms
Rate Negotiation
Rate Negotiation

BFD has two main operating modes: Asynchronous and Echo mode.

3.2.2 BFD Asynchronous Mode

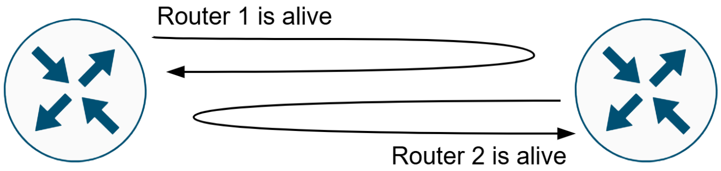
In Asynchronous mode BFD sends control packets in every direction informing the adjacent node that it is alive.



These control packets are sent periodically, if a number of packets (default is 3) is not received the adjacent node assumes there’s a link or forwarding plane problem and the session is declared terminated.

3.3 BFD Echo Mode

In Echo mode BFD sends packets to its own IP address, packets then are sent to the adjacent node and sent back.



As in the previous case, the packets are sent in a periodic way and a number of lost packets will cause the session to be considered down; the benefit of the echo mode is that it also tests the forwarding plane of the remote node.

In both modes BFD notifies the routing process immediately when the interface is down and it does it before the hello and hold timers expire.

The supported mode and the one to be implemented is BFD Echo mode. The recommendation is to use it on the links between the sites that don't use transmission media.

3.3.1 BFD in OSPF

It is recommended to implement BFD on a per OSPF interface basis for links that are not considered a dark fiber.

BFD in OSPF configuration – IOS

```
!
interface <interface-id>
 bfd interval 100 min_rx 100 multiplier 4
!

Table 45: BFD in OSPF configuration – IOS XE
!
interface <interface-id>
 bfd interval 100 min_rx 100 multiplier 4
!
```

BFD in OSPF configuration – IOS-XR

```
!
router ospf 1
 bfd interval 100
 bfd multiplier 4
 area 0
  interface <interface-id>
   bfd fast-detect
  !
 !
!
```

3.3.2 Carrier-Delay Interface

This delay specifies the time in which the operative system allows an interface to change its state and return to the initial state without notifying the interface is down (this is called debouncing). The default time is 2 seconds and the optimization of this parameter is crucial in a fast convergence environment, and the recommended configuration is 0ms for "down" and 500ms for "up".

Carrier-delay configuration – IOS / IOS-XE

```
!
interface <interface-id>
 carrier-delay down msec 0
 carrier-delay up msec 500
!
```

Carrier-delay configuration – IOS-XR

```
!
interface <interface-id>
 carrier-delay up 500 down 0
!
```

3.3.3 IP Routing Protocol Purge Interface

The "ip routing protocol purge interface" IOS command allows the routing protocols to remove the independent routes from the RIB when a link on the router goes down and the interface is removed from the routing table.

If this command is not used and the link goes down, the less efficient of the RIB is called automatically to eliminate all the prefixes from the RIB that have this interface as next-hop. When the process runs over a big routing table, it can consume several CPU cycles and increase the convergence time.

IP Routing Protocol Purge Interface configuration – IOS

```
!
ip routing protocol purge interface
!
```

3.4 At a Service Level

3.4.1 Hot Standby Router Protocol (HSRP)

A LAN client can use a dynamic process or static configuration to determine which router should be its gateway (first hop) to reach a remote destination in particular. Some examples of protocols for dynamic discovery on a router are:

- Proxy ARP. The client uses ARP to reach the destination it wants and the router responds to the ARP request with its own MAC address.
- Routing Protocols. The client listens to the dynamic routing protocols and builds its own routing table.
- IRDP (ICMP Router Discovery Protocol). The client runs the ICMP protocol to discover a router.

The disadvantage of dynamic protocols for discovery is that they require configuration and generate an increase on the LAN client processing. Also, in case of a failure in the router, the process of commuting to another router can be somehow slow.

An alternative to dynamic protocols is to configure the default gateway statically in the client. This way simplifies the configuration in the client and the processing, but it creates a single point of failure. If the default gateway fails, the LAN client's communication is limited since only local communication works but the connectivity to the rest of the network is reduced.

This protocol establishes a framework between network routers in order to achieve default gateway failover if the primary gateway becomes inaccessible, in close association with a rapid-converging routing protocol like EIGRP or OSPF. HSRP routers send multicast Hello messages to other routers to notify them of their priorities (which router is preferred) and current status (Active or Standby).

The primary router with the highest configured priority will act as a virtual router with a pre-defined gateway IP address and will respond to the ARP / ND request from machines connected to the LAN with a virtual MAC address. If the primary router should fail, the router with the next-highest priority would take over the gateway IP address and answer ARP requests with the same MAC address, thus achieving transparent default gateway failover.

HSRP configuration – IOS / IOS-XE

```
!
interface <interface-id>
 ip address <ip address>
 standby version 2
 standby <id> priority <priority>
 standby <id> preempt
 standby <id> ip <virtual ip address>
!
```

HSRP configuration – IOS-XR

```
!
router hsrp
 interface <type> <interface-path-id>
  address-family ipv4
   hsrp <id> version 2
   address <virtual ip address>
   priority <priority>
   preempt
!
```

3.4.2 Virtual Router Redundancy Protocol (VRRP)

VRRP is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails.

VRRP configuration – IOS / IOS-XE

```
!
interface <interface-id>
 ip address <ip address>
 vrrp <id> priority <priority>
 vrrp <id> ip <virtual ip address>
 vrrp <id> preempt
!
```

VRRP configuration – IOS-XR

```
!
router vrrp
 interface <type> <interface-path-id>
 address-family ipv4
  vrrp <vrid> version { 2 | 3 }
  address <virtual ip address>
  preempt
!
```

3.4.3 Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol is a standard protocol that runs over Layer 2 in all Routers and Switches. In the Service Provider network, LLDP should be configured only in the ports connecting to devices in the MPLS Core; ports connecting toward Customers should not run LLDP to avoid leaking infrastructure information to any third party.

LLDP configuration - IOS / IOS-XR / IOS-XR

```
!
interface <interface-id>
 no lldp enable
!
```

3.5 Recommendations for High Availability

In order to keep high availability in the network, the following recommendations are mentioned:

- It is very important to keep Stateful Switchover (SSO) in all devices that maintain redundancy of route processors. In case of failure, manual or automatic switchover could immediately reestablish the control plane avoiding large periods of downtime.
- In platforms working with distributed architecture non – stop forwarding is recommended to keep the packet forwarding in case of a failure occurs in the control – plane. Data plane keeps the forwarding of packets during reestablishment of a Route Processor or while Standby Route Processor is taking the primary role.
- To accelerate the convergence of the network, BFD configuration is recommended. When a BFD session between neighbors is lost, Bidirectional Forwarding Detection triggers messages which announces to the IGP that flood or convergence should be initiated.

- Configuring IP Event Dampening improves the convergence times and the stability of the network by isolating failures, if they are not propagated, which also reduces the use of processing resources from other devices in the network. When interfaces are flapping, IP Event Dampening suppresses links flapping and keeps network stability.

4 Network Management

This section contains configurations specific to network management that will be implemented on the network devices.

4.1 SNMP

SNMP configuration is required to allow the management systems to monitor the general status of the network devices.

The Simple Network Management Protocol (SNMP) is used to gather statistics, counters and tables stored in a network device. The information gathered can be used for Network Management Stations (NMS) to generate real time alerts, measure availability and provide capacity planning information, as well as to help perform configurations and checkups for troubleshooting.

The SNMP register sends notifications about significant changes in the system status to the management stations of SNMP. It is recommended to permit the SNMP traps for the event logging.

SNMP configuration – IOS

```
!
ip access-list standard <ACL name>
 permit <ip_address>
!
snmp-server community <community read only> RO <ACL name>
snmp-server community <community write> RW <ACL name>
snmp-server source-interface trap <source Loopback>
snmp-server location <router_location>
snmp-server ip dscp 48
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps tty
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bfd
snmp-server enable traps bgp
snmp-server enable traps bgp cbgp2
snmp-server enable traps config-copy
snmp-server enable traps config
```

```
snmp-server enable traps ipsla
snmp-server enable traps memory bufferpeak
snmp-server enable traps cpu threshold
snmp-server enable traps cef resource-failure peer-state-change
peer-fib-state-change inconsistency
snmp-server enable traps resource-policy
snmp-server enable traps flash insertion removal
snmp-server enable traps netsync
snmp-server enable traps rsvp
snmp-server enable traps aaa_server
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps pw vc
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps alarms informational
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps rf
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps mac-notification
snmp-server enable traps mpls vpn
snmp-server enable traps mpls rfc vpn
!
```

SNMP configuration – IOS-XR

```
!
ipv4 access-list <ACL-name>
 10 permit ipv4 host <ip-address> any
!
snmp-server ifindex persist
snmp-server host <ip-address>
snmp-server community <community_name> RO <ACL-name>
snmp-server community <community_name> RW <ACL-name>
!
snmp-server traps rf
snmp-server traps bfd
snmp-server traps ethernet cfm
snmp-server traps ntp
snmp-server traps ethernet oam events
snmp-server traps copy-complete
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
snmp-server traps snmp coldstart
snmp-server traps snmp warmstart
snmp-server traps snmp authentication
snmp-server traps flash removal
snmp-server traps flash insertion
snmp-server traps config
snmp-server traps entity
snmp-server traps selective-vrf-download role-change
```

```
snmp-server traps syslog
snmp-server traps system
snmp-server traps ospf lsa lsa-maxage
snmp-server traps ospf lsa lsa-originate
snmp-server traps ospf errors bad-packet
snmp-server traps ospf errors authentication-failure
snmp-server traps ospf errors config-error
snmp-server traps ospf errors virt-bad-packet
snmp-server traps ospf errors virt-authentication-failure
snmp-server traps ospf errors virt-config-error
snmp-server traps ospf retransmit packets
snmp-server traps ospf retransmit virt-packets
snmp-server traps ospf state-change if-state-change
snmp-server traps ospf state-change neighbor-state-change
snmp-server traps ospf state-change virtif-state-change
snmp-server traps ospf state-change virtneighbor-state-change
snmp-server traps bridgemib
snmp-server traps entity-state operstatus
snmp-server traps entity-state switchover
snmp-server traps entity-redundancy all
snmp-server traps entity-redundancy status
snmp-server traps entity-redundancy switchover
snmp-server trap-source Loopback0
snmp-server traps mpls frr all
snmp-server traps mpls ldp up
snmp-server traps mpls ldp down
snmp-server traps mpls ldp threshold
snmp-server traps mpls l3vpn all
snmp-server traps mpls l3vpn vrf-up
snmp-server traps mpls l3vpn vrf-down
snmp-server traps mpls l3vpn max-threshold-cleared
snmp-server traps mpls l3vpn max-threshold-exceeded
snmp-server traps mpls l3vpn mid-threshold-exceeded
snmp-server traps mpls l3vpn max-threshold-reissue-notif-time 1
snmp-server traps pim neighbor-change
snmp-server traps pim invalid-message-received
snmp-server traps pim rp-mapping-change
!
```

4.2 Syslog

To assist and simplify the problem resolution and the security investigations, it is necessary to monitor the information generated by the router. In its simplest form, this can be achieved by using the information stored in the buffer memory. To make the logging system useful, the default buffer size should be increased.

Although it is simple, this method has some disadvantages:

- It is volatile. The information in the buffer does not survive if the system is rebooted.

- Has a limited capacity. The volume of information that can be stored in the buffer is directly related to the amount of memory of the system and the portion of it that is reserved to do so.
- The configuration of the buffer will mean a decrease in resources from the router's central functions.

It is recommended that the logging structure is based on a syslog infrastructure. This allows the device to register physically and even geographically to a separate system using syslog. Multiple syslog servers can be configured for redundancy and information distribution.

When a basic logging is configured, it is a good practice to disable console logging. Console logging can be enabled when required.

Syslog configuration – IOS

```
!
no logging console
logging monitor informational
!
logging buffered 100000
!
logging trap debugging
logging source-interface <source Loopback>
logging <server>
!
```

Syslog configuration – IOS-XR

```
!
logging trap debugging
logging events display-location
logging history critical
no logging archive
!
logging <ip-address> vrf default severity info
logging source-interface <mgmt-loopback>
!
service timestamps log datetime localtime msec
service timestamps debug datetime localtime msec show-timezone
service timestamps log uptime
!
logging console disable
!
```

5 Network Operation

5.1 General Security

In IOS-XR most of the services that used to be disabled in IOS are already disabled. However it is recommendable to disable the following service:

5.1.1 IP Domain Lookup

IP Domain Lookup looks for name resolution every time an unknown string is entered in the CLI. This lookup can take several minutes depending on the DNS reachability.

IP Domain Lookup services configuration – IOS / IOS-XE

```
!
no ip domain-lookup
!
```

IP domain lookup Services disabling – IOS-XR

```
!
ip domain-lookup disable
!
```

5.1.2 Finger Service

Finger is used to find out which users are registered in a network device. Although this information is not highly sensitive, it can sometimes be useful in case of attacks. Also, the Finger service can be used in a specific type of Denial of Service (DoS) attack called Finger of Death, which implies sending a Finger request to a specific system every minute, but never disconnecting.

No Service Finger configuration – IOS

```
!
no service finger
!
```

5.1.3 PAD Service

The security audit disconnects all the commands of the assemble/disassemble packets (PAD) and the connections between PAD devices and access servers whenever possible.

No Service PAD configuration – IOS / IOS-XE

```
!
no service pad
!
```

5.1.4 Nagle Service

When a standard TCP implementation is used to send key strokes between machines, the TCP is used to send a packet for every key pressed. In bigger networks, lots of small packets use too much bandwidth and contribute to congestion.

The algorithm developed by John Nagle (RFC 896) helps to alleviate the small packet problem in TCP. Generally, it works the following way: The first key pressed after the connection is established is sent in a unique packet, but TCP holds any additional character pressed until the receiver acknowledges the previous packet. Then the second largest packet is sent and any additional character is kept until the return of the acknowledgement. The effect is to group characters in bigger parts and control their travel through the network according to the time taken to arrive and to return on a specific connection. This feature is enabled by default on IOS-XR.

Nagle Service configuration – IOS

```
!
service nagle
!
```

5.1.5 Service Password Encryption

This encrypts all the passwords, including the username, console, and VTY line and authentication keys for routing protocols. However, it must be pointed out that the cipher used is only to prevent that the passwords are seen on a configuration file. The configuration files with encrypted passwords can be easily deciphered using public domain tools.

Service Password Encryption configuration – IOS / IOS-XE

```
!
service password-encryption
!
```

5.1.6 TCP Keepalives for Inbound

To generate keepalive packets for inactive inbound connections (initiated by a remote device), the command "service tcp-keepalives-in" is used in global configuration mode.

TCP Keepalives for Inbound configuration – IOS

```
!
service tcp-keepalives-in
!
```

5.1.7 TCP Keepalives for Outbound

To generate keepalive packets for inactive outbound connections (initiated by a user), the command "service tcp-keepalives-out" is used in global configuration mode.

TCP Keepalives for Outbound configuration – IOS

```
!
service tcp-keepalives-out
!
```

5.1.8 TCP Small Servers Service

By default, the TCP Small Servers (Echo, Discard, Chargen and Daytime) are disabled. If disabled, the access to these ports causes the Cisco IOS Software to send a TCP RESET packet to the source and discard the original incoming packet.

TCP Small Servers Service configuration – IOS

```
!
no service tcp-small-servers
!
```

5.1.9 UDP Small Servers Service

By default, Cisco devices with an IOS 11.3 release or below offer the small services: echo, charge and discard. These services, especially in their UDP versions are rarely used for legitimate purposes but can be used to send DoS packets and other attacks that otherwise would be prevented by packet filtering.

Even though most of the attacks can be avoided or made less hazardous using anti spoofing access lists, the best policy is to disable them in all the routers.

UDP TCP Small Servers Service configuration – IOS

```
!
no service udp-small-servers
!
```

5.1.10 DHCP Service

Disabling the DHCP service or relay agent on the devices will mitigate the vulnerability to DoS attacks such as the “Blocked input-queue”.

The command to disable the DHCP service in a device is:

DHCP Service configuration – IOS

```
!
no service dhcp
!
```

5.1.11 Sequence Numbers and Time Stamps

The time stamps and logging messages indicate the date and time in which the message was generated. The sequence numbers indicate the sequence in which the messages with identical time stamps were generated. Knowing this is an important tool in diagnosing potential attacks,

Sequence Numbers and Time Stamps configuration – IOS / IOS-XE

```
!
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
service sequence-numbers
!
```

Sequence Numbers and Time Stamps configuration – IOS-XR

```
!
service timestamps log datetime localtime msec show-timezone
service timestamps debug datetime localtime msec show-timezone
!
```

5.1.12 IP Identification Service

The identification support allows asking a TCP port for identification. This feature permits a guarantee-less protocol to report the identity of a client that is initiating a TCP connection and of a host that is replying for that connection. With identification support, you can connect a host to a TCP port and send a simple text line to ask for information and receive a simple text line in response.

It is dangerous to allow any system in a segment directly connected that learns that the router is a Cisco device and determine the model number and software version it is using. This information can be used to design attacks against this router.

IP Identification Service configuration – IOS

```
!
no ip identd
!
```

5.1.13 IP HTTP/HTTPS Server

The IOS and IOS-XE routers have an HTTP/HTTPS server. This must be disabled:

HTTP/HTTPS Server configuration – IOS / IOS-XE

```
!
no ip http server
no ip http secure-server
!
```

5.1.14 Enable Secret

It is recommended to use the command “enable secret” instead of “enable password”. The cypher algorithm type 7 used with the command enable password and service password encryption is reversible. The command enable secret provides a better security storing the secret password using a non-reversible cryptographic function. The cypher layer added to the security is useful in environments where the password travels across the network or it is stored in a TFTP server.

Enable Secret configuration – IOS / IOS-XE

```
!
service password-encryption
enable secret <enable_secret>
```

```
no enable password
!
```

5.1.16 VTY Access

It is recommended to enable SSH as the only valid protocol on the VTY lines. The following template can be used:

VTY Access configuration - IOS

```
!
access-list <ACL-number> permit <ip_address>
access-list <ACL-number> deny any log-input
!
line vty 0 100
 exec-timeout 5 0
 access-class <ACL-number> in
 transport input ssh
 transport output ssh
!
```

VTY Access configuration – IOS-XR

```
!
line default
 password <password>
 exec-timeout 5 0
 access-class ingress <vty-ACL-name>
 session-timeout 30
!
line template <line-template-name>
 exec-timeout 5 0
 access-class ingress <vty-ACL-name>
 session-timeout 30
 transport input ssh
!
vty-pool default 0 100 line-template <line-template-name>
!
ipv4 access-list <vty-ACL-name>
 10 permit ipv4 host <ip_address> any
 20 deny ipv4 any any log-input
!
```

5.2 NTP

Synchronous timing is a crucial necessity for network environments nowadays. Each aspect of management, security, planning and troubleshooting of a network includes determining when the events occur. Time is a vital element that permits an event in a node to be mapped to a corresponding event in another one.

NTP configuration – IOS / IOS-XE

```
!
clock timezone {timezone}
!
ntp source <mgmt-loopback>
ntp update-calendar
ntp server <ip-address>
!
```

NTP configuration – IOS-XR

```
!
clock timezone {timezone}
!
ntp
 authenticate
 source <mgmt-loopback>
 update-calendar
 server <ip-address>
 access-group ipv4 peer <ACL-name>
!
ipv4 access-list <ACL-name>
 10 permit ipv4 host <ip-address> any
!
```

5.3 FTP

It is highly advisable to define explicitly the source FTP interface to be used for any FTP session. The following configuration is required:

FTP configuration – IOS / IOS-XE

```
!
ip ftp source-interface <mgmt-loopback>
!
```

FTP configuration – IOS-XR

```
!
ftp client source-interface <mgmt-loopback>
!
```

5.4 SSH – Secure Shell

Secure Shell (SSH) is recommended as the method to use for network devices management. It is also recommended to limit the virtual console access to avoid unauthorized users to access the network devices.

SSH configuration – IOS / IOS-XE

```
!
hostname <hostname>
ip domain name {domain-name}
ip ssh version 2
!
```

SSH configuration – IOS-XR

```
!
hostname <hostname>
domain name {domain-name}
ssh server v2
ssh server session-limit 10
ssh timeout 10
ssh server logging
ssh server enable
!
```

5.5 AAA

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. These three function are:

- **Authentication**: Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.
- **Authorization**: Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, etc.
- **Accounting**: Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands, number of packets, and number of bytes, etc.

AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions.

5.5.1 AAA Accounting for commands

Accounting should be configured using the default or a named method, for each level of user access to network devices. Customers who have more stringent security requirements, may want to implement additional levels such as 1, 7, and 15 for increasing levels of command access.

AAA Accounting for commands configuration – IOS / IOS-XE / IOS-XR

```
!
aaa accounting exec default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa accounting commands default start-stop group tacacs+
aaa accounting commands 1 start-stop group tacacs+
aaa accounting commands 15 start-stop group tacacs+
aaa accounting update periodic 2
!
```

5.6 TFTP

The Trivial File Transfer Protocol (TFTP) is used to copy configuration files and operative systems from and to the router. It is only required to configure the following:

TFTP configuration – IOS / IOS-XE

```
!
ip tftp source-interface <mgmt-loopback>
!
```

TFTP configuration – IOS-XR

```
!
tftp client source-interface <mgmt-loopback>
!
```

5.7 Management Plane Protection (MPP)

This functionality allows filtering the management access to the IOS-XR, CRS and ASR9k devices. The Telnet, SSH and SNMP connections will be limited.

Management Plane Protection (MPP) configuration – IOS-XR

```
!
control-plane
```

```
 management-plane
  inband
   interface all
    allow TELNET peer
     address ipv4 X.Y.A.0/24
    !
    allow SSH peer
     address ipv4 X.Y.B.0/24
    !
    allow SNMP peer
     address ipv4 X.Y.C.0/24
    !
   !
  !
 !
!
```

5.8 Recommendations for General Security and Management

In order to follow with the best practices for the network many recommendations can be mentioned:

- Time stamps should be enabled to have timed logs messages which help for troubleshooting
- Management through http or https must be disabled in all platforms to avoid any type of attack by using TCP 80 and 443 ports.
- To increment security in the remote access it is recommended to enable access - list to protect the line templates (IOS-XR) and line vty (IOS). Additionally MPP should be configured to have redundant protection in the management plane for IOS-XR platforms so in case of involuntary disabling of access list, MPP could protect the platform.
- NTP should be protected by password encryption.
- It is recommended to modify the initial value of the TCP window from 4128 to 65535 bytes. The TCP window size increase reduces the TCP/IP overhead by lowering the quantity of ACKs in the network, helping other functionalities that use TCP to converge faster. This feature applies to the TCP sessions that start or end in an IOS-XR device
- As it is recommended to use “PMTUD”, it is necessary to take care about “ip icmp unreachable”, because ICMP unreachable response is a prerequisite for PMTUD to work.
- It is recommended to use SSHv2 to access all the devices in the MPLS network. SSHv2 is a secure method because it sends encrypted sessions between devices.

6 Miscellaneous

6.1 Login Banner

When a connection to a network device is open, a logging banner will be displayed. The banner must state that unauthorized personnel don’t have access to the device and should give no information about the device’s location or owners to protect the infrastructure and the business from malicious users.

Login Banner configuration – IOS / IOS-XE

```
!
banner login ^
*****************************************************************************
*                                                                           *
*           THIS SYSTEM IS FOR THE USE OF AUTHORISED USERS ONLY!            *
*                                                                           *
*                                                                           *
*     For unauthorized users all access is prohibited and protected by      *
*     international law. Individuals using this system are subject to       *
*     having all of their activities on this system monitored and           *
*     recorded by systems and personnel.                                    *
*                                                                           *
*     When you login to this network you automatically agree with the       *
*     above mentioned terms!                                                *
*                                                                           *
*     Disconnect IMMEDIATELY if you are not an authorised user!             *
*                                                                           *
*                                                                           *
*****************************************************************************
^C
!
```

Login Banner configuration – IOS-XR

```
!
banner login ^
*****************************************************************************
*                                                                           *
*           THIS SYSTEM IS FOR THE USE OF AUTHORISED USERS ONLY!            *
*                                                                           *
*                                                                           *
*     For unauthorized users all access is prohibited and protected by      *
*     international law. Individuals using this system are subject to       *
*     having all of their activities on this system monitored and           *
*     recorded by systems and personnel.                                    *
*                                                                           *
*     When you login to this network you automatically agree with the       *
*     above mentioned terms!                                               *
*                                                                          *
*     Disconnect IMMEDIATELY if you are not an authorised user!            *
*                                                                          *
*                                                                          *
****************************************************************************
^C
!
```

6.2 Exec Banner

After a successful login, a second banner can be displayed stating that the device belongs to a specific company. It’s recommended to add useful information such as:

- Hostname
- Device location
- Support contact information
- Warnings

Exec Banner configuration – IOS/IOS-XE/IOS-XR

```
!
banner exec  ^
**********************************************************
*                                                        *
*  THIS SYSTEM IS FOR THE USE OF AUTHORISED USERS ONLY!  *
*                                                        *
*       This node is property of {company-name}          *
*          Hostname:    {hostname}                       *
*          Location:    {site},{rack}                    *
*          Contact:     {email-address}                  *
*                                                        *
*    Hardware or software changes in this device         *
*   can only be performed by authorized personnel        *
*                                                        *
**********************************************************
^C
!
```

6.3 Source Interface for network operations

For network operations, the use of the same interface for all the services is recommended. For every device in the infrastructure, the management Loopback interface should be used, adding the commands below. Some commands have been covered previously in this document, but have been included again here for completion purposes.

Source interface configuration – IOS / IOS-XE

```
!
snmp-server trap-source <mgmt-loopback>
ip telnet source-interface <mgmt-loopback>
ip ssh source-interface <mgmt-loopback>
ip tftp source-interface <mgmt-loopback>
ip ftp source-interface <mgmt-loopback>
logging source-interface <mgmt-loopback>
ntp server <server> source <mgmt-loopback>
ip tacacs source-interface <mgmt-loopback>
!
```

Source interface configuration – IOS-XR

```
!
logging source-interface <mgmt-loopback>
!
telnet ipv4 client source-interface <mgmt-loopback>
ssh client source-interfac <mgmt-loopback>
tftp client source-interface <mgmt-loopback>
ftp client source-interface <mgmt-loopback>
tacacs source-interface <mgmt-loopback>
!
snmp-server trap-source <mgmt-loopback>
!
ntp
 server <address> source <mgmt-loopback>
!
```

6.4 Duplicate IP addresses Policy

In IOS-XR, by default, if an IPv4 or IPv6 address is configured on an interface and that address conflicts with another address already configured, anywhere else within the chassis, then the interface with the lower number rack/slot/port will become active, and the interface with the higher number rack/slot/port will be inactive (line protocol will be down).

This can lead to a situation where an accidental configuration on an interface brings down an already active interface, if the accidental configuration is done on an interface numbered with a lower rack/slot/port. To maintain the existing interface numbering and to put any new interface that conflicts with an existing one in a line protocol down state, configure the command below in global mode; this enables the Address Repository Manager conflict resolution (IPARM).

Duplicate IP Address Policy – IOS-XR:

```
!
ipv4 conflict-policy static
!
```

6.5 TCP Optimizations

All TCP sessions are limited by the number of bytes that can be transported on a packet. This limit known as Maximum Segment Size (MSS) is 536 bytes by default. Enabling the Path MTU Discovery (PMTUD) feature enables the TCP protocol to determine the smallest MTU size across all the links that the TCP session uses. This protocol then uses this MTU value, without the space for the IP and TCP headers as MSS of the session.

The MSS increase reduces the TCP/IP overhead, helping other functionalities that use TCP to converge faster.

TCP Optimizations configuration – IOS, IOS XE and XR:

```
!
tcp path-mtu-discovery
tcp window-size 65535
!
```

7 Next Steps

I hope you find this document very useful!

I invite you to review the OSPF and MPLS LDP best practices presented here, identify which recommendations best fit your network scenario, and apply them to optimize your infrastructure.

If you need personalized assistance for design, implementation, or optimization of your network, feel free to contact me. You can send me a direct message via LinkedIn at linkedin.com/in/pdiazd or email me at contact@pdiazd.com.

Sincerely,

Pablo Díaz
Senior Network Engineer, Founder @Pragmático
contact@pdiazd.com
linkedin.com/in/pdiazd