Module 11 – Advanced Router Configuration

Objective: Create a basic physical lab interconnection with two autonomous systems. Each AS should use OSPF, iBGP and eBGP appropriately to construct a working network.

Prerequisites: Basic ISP Workshop (at least Modules 1 to 8)

The following will be the common topology used.

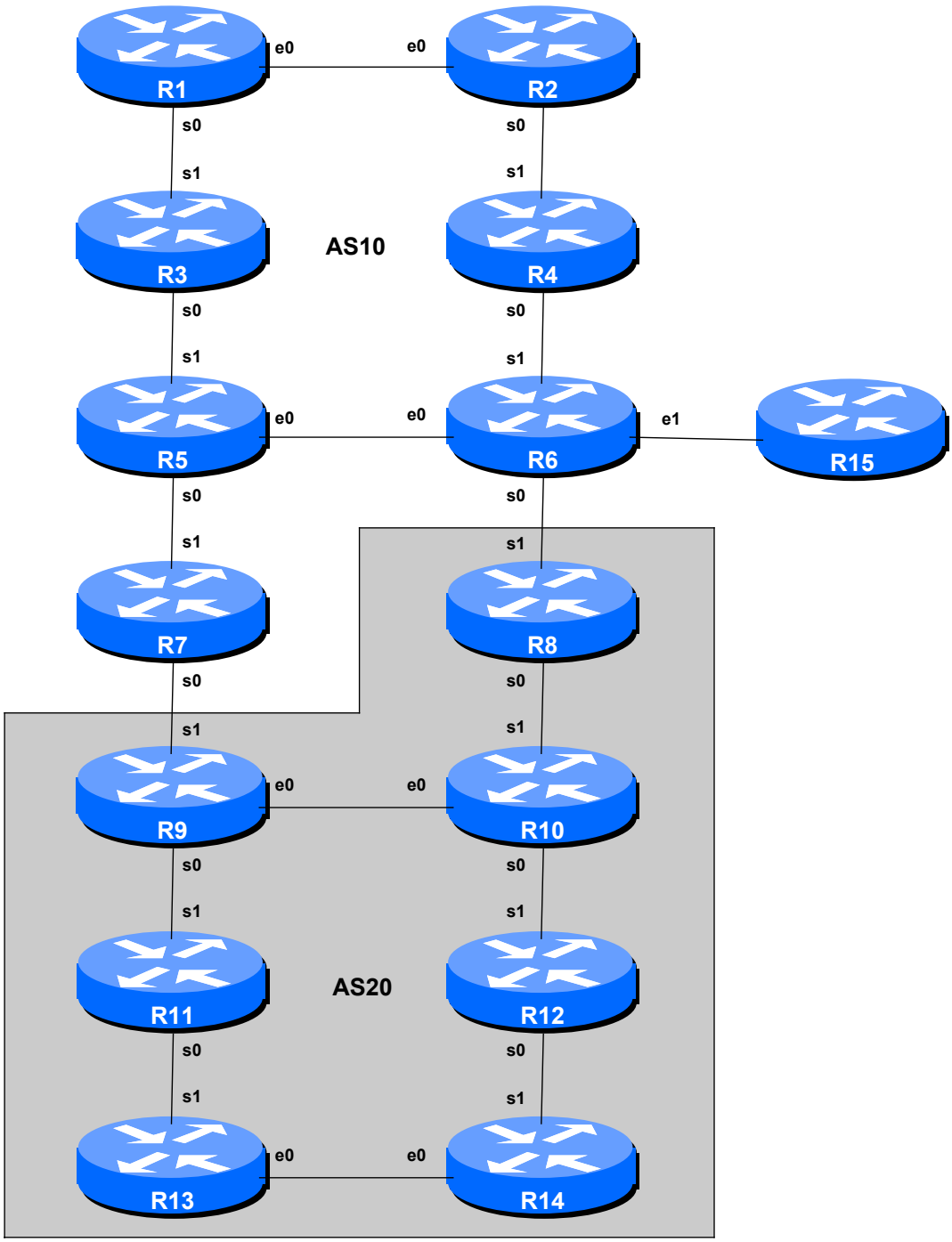


Figure 1 – ISP Lab Basic Configuration

Lab Notes

The purpose of this module is to construct the workshop lab and introduce participants to IOS 12.0S. It should serve as a reminder on the basic principles of building a network, introducing an IGP, properly function iBGP, and the basics of eBGP:

- After the **physical design** is established, the connections between the hardware should be built and verified.

- Next, the routers should have the **base configuration** installed, and basic but sufficient security should be set up. Note that Router15 is the Workshop Instructor's router and it will be used at various instances throughout the workshop.

- Next the **basic IP connectivity** be tested and proven. This means assigning IP addresses on all links which are to be used, and testing the links to the neighbouring devices.

- Only once one router can see its neighbour does it make sense to start configuring routing protocols. And **start with the IGP** (OSPF is chosen for this workshop). There is no purpose to building BGP while the chosen IGP (in this case OSPF) is not functioning properly. BGP relies on OSPF to find its neighbours and next hops, and an improperly or non-functioning OSPF will result in much time wasted attempting to debug routing problems.

- Once the IGP is functioning properly, the **BGP configuration** can be started, first internal BGP, then external BGP.

- Finally, **documentation**. Documentation is often overlooked or forgotten. It is an ongoing process in this workshop. If the instructor asks you to document something, either on the whiteboard in the class, or at the back of this booklet, it is in your best interests to do so. There can never be too much documentation, and documentation at the time of network design and construction can usually saves much frustration at a future date or event.

Lab Exercise

The following list is typical for what needs to be done to bring up the lab configuration:

1. **Router Hostname.** Each router will be named according to the table location, Router1, Router2, Router3, etc. Documentation and labs will also refer to *Router1* as R1.

```
hostname Router1
```

2. **Turn Off Domain Name Lookups.** Cisco routers will always try to look up the DNS for any name typed on the command line. You can see this when doing a *trace* on a router with no DNS server or a DNS server with no in-addr.arpa entries for the IP addresses. Unless the Workshop Instructor specifically tells you that there is a nameserver configured for the lab, we will turn this lookup off for the labs to speed up traceroutes.

```
no ip domain-lookup
```


Cisco Systems Inc
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

3. **Disable Command-line Name Resolution.** The router by default attempts to use the various transports it supports to resolve the commands entered into the command line during normal and configuration modes. If the commands entered are not part of Cisco IOS, the router will attempt to use its other supported transports to interpret the meaning of the name. For example, if the command entered is an IP address, the router will automatically try to connect to that remote destination. This feature is undesirable on an ISP router as it means that typographical errors can result in connections being attempted to remote systems, or time outs while the router tries to use the DNS to translate the name, and so on.

```
line con 0
 transport preferred none
line vty 0 4
 transport preferred none
```

4. **Usernames and Passwords.** All router usernames and passwords should be ***cisco***. Please do **not** change the username or password to anything else, or leave the password unconfigured (access to vty ports is not possible if no password is set). It is essential for a smooth operating lab that all participants have access to all routers.

```
username cisco password cisco
enable secret cisco
service password-encryption
```

   The *service password-encryption* directive tells the router to encrypt all passwords stored in the router's configuration (apart from *enable secret* which is already encrypted).

   Note that while we use username *cisco* and many instances of a password of *cisco* in these workshops, under no circumstances must any service provider operator ever use easily guessable passwords as these on their live operational network[1].

5. **Enabling login access for other teams.** In order to let other teams telnet into your router, you need to configure a password for all virtual terminal lines.

```
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
```

   This series of commands tells the router to look locally for standard user login (the username password pair set earlier), and to the locally configured enable secret for the enable login. By default, login will be enabled on all vtys for other teams to gain access.

6. **Configure system logging.** A vital part of any Internet operational system is to record logs. The router by default will display system logs on the router console. However, this is undesirable for Internet operational routers, as the console is a 9600 baud connection, and can place a high processor interrupt load at the time of busy traffic on the network. However, the router logs can also be recorded into a buffer on the router – this takes no interrupt load and it also enables to operator to check the history of what events happened on the router. In a future module, the lab will configuration the router to send the log messages to a SYSLOG server.

[1] This sentence cannot be emphasized enough. It is quite common for attackers to gain access to networks simply because operators have used familiar or easily guessed passwords.

```
no logging console
logging buffered 8192 debugging
```

which disables console logs and instead records all logs in a 8192byte buffer set aside on the router.

7. **CIDRise the router.** Make sure the router is configured for CIDR. These two commands are now default in 12.0S, but it is good practice to check just in case:

```
ip subnet-zero
ip classless
```

8. **Set up timestamps for all logs on the router.** 12.0S has made basic timestamping on the logs the default but ISPs should enable the complete detail on their logs as follows:

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

Refer to IOS Essentials or the router's on-line help system if you have forgotten what these options mean.

9. **Set up a login banner.** Next, set up a login banner. Use an appropriate greeting – consult IOS Essentials document for appropriate and inappropriate greetings. If you use an inappropriate greeting, expect the lab instructors to ask you to change it. For example

```
banner login ^
Cisco Systems BGP Multihoming Workshop Lab
^
```

10. **Tidy up the vty and console interface configuration.** In the real world we'd now add access-lists to the vty ports on the router. However, this lab is not connected to any external network or the Internet so these will not be required. However, we need to make some changes to the defaults. Basically, only telnet will be the supported mechanism to connect to the routers, and only telnet will be the permitted mechanism to connect from one router to the next.

```
line vty 0 4
 transport input telnet
 transport output telnet
```

11. **Create a loopback interface.** Loopback interfaces will be used in this workshop for many things. They are an essential and fundamental requirement for any ISP backbone:

```
interface loopback 0
 description Loopback Interface for RouterXX
```

12. **Disable pad, finger and bootp servers.** The pad, finger and bootp servers are running by default in IOS. These should be disabled on any Internet router. Finger is a security risk, bootp and pad are simply unnecessary.

```
no service pad
no ip finger
no ip bootp
```

13. **Remove unneeded SNMP configuration.** IOS versions prior to 12.0S install a default SNMP configuration when the router first starts with an unconfigured NVRAM. As we will not be using SNMP to access the routers in the workshop, check if the SNMP configuration is there and remove it if it is. (Unless configured correctly SNMP is a security risk in the Internet.) Example:

```
no snmp-server community public
```

14. **Time synchronisation.** Router 15 in Figure 1 will always be connected to the workshop network in some way described by the workshop instructors. Its IP address will always be 192.168.1.1/24. And it will be running as a time source with address 192.168.1.2. You should configure ntp to peer with that router, so that the time on your router is synchronised with it and those in the rest of the lab. Don't forget to set the timezone. For example:

```
clock timezone SST 8     ! Singapore Standard Time is GMT+8
ntp server 192.168.1.2
```

15. **Enable CEF.** Router platforms from the 2600 upwards support CEF. Those teams with capable hardware should enable CEF now. Note that CEF is neither supported nor available on the 2500 series.

```
ip cef
```

    Entering the *sh cef interface* command will show the status of CEF on the router interfaces. And the command *sh ip cef* will show the forwarding table – currently empty.

16. **Saving the configuration.** With the basic configuration in place, save the configuration by using "write memory". Then log off the router by typing exit, and then log back in again. Notice how the login sequence has changed, prompting for a "username" and "password" from the user. Don't forget to frequently save the configuration to NVRAM after each configuration change.

    IMPORTANT NOTE: Each router team is strongly recommended to make a copy of the basic router configuration at this stage. It will be assumed throughout this workshop that the above configuration will **ALWAYS** be present on the router. If it is not, each router team will be requested to restore it as a matter of urgency.

Checkpoint #1: *call lab assistant to verify the connectivity. Save the configuration as it is on the router either on the worksheet on the end of this hand out, or own your own laptop, or on the classroom tftp server if it is available. It will be required again several times throughout this workshop.*

17. **Back to Back Serial Connections.** Connect the serial connections as in Figure 1. The DCE side of a back to back serial connection is configured with the *clock rate* command that drives the serial circuit.

```
interface serial 0/0
 description DCE Serial Connection to RouterXX
 clock rate 2000000
!
```

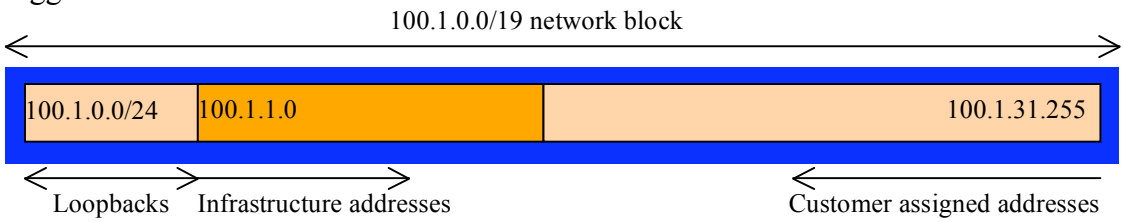
18. **Ethernet Connections.** Use the Catalyst 2924XLs to interconnect the routers using ethernet. *Straight* RJ-45 cables will be used to connect the routers to the switches. The switches will have been configured for multiple vLANs. Ask the instructor if there is doubt as to what the vLAN ranges are.

19. **IP Addresses.** Each AS is assigned a block of IP addresses.

    AS10 100.1.0.0/19 AS20 100.2.0.0/19

    Decide among your team what the addressing plan for you AS should be.
    Hint One: point to point links only require /30 blocks.
    Hint Two: loopbacks only require a /32 host address.
    Hint Three: number your backbone sequentially, from either the start or finish of the range.

    Suggestion:



    Note: When the IP addresses are assigned, they **MUST** be annotated on the **WHITE-BOARD** at the front of the workshop room. A large network map will have been drawn on the white-board – all the IP address assignments need to be annotated there so that other Router Teams can document and understand the links and routing in this and future modules.

20. **Ping Test #1.** Ping all physically connected subnets of the neighbouring routers. If the physically connected subnets are unreachable, consult with your neighbouring teams as to what might be wrong. Don't ignore the problem – it may not go away.

21. **OSPF within the same AS.** Each router Team should enable OSPF on their router. The OSPF process identifier should be the same as your AS number. All the routers in one AS will be in OSPF Area 0. Use a network statement for every connected interface. Also, use a network statement for the loopback interface address but with a host mask. Don't forget to mark the loopback interface as a passive interface – for example:

```
router ospf 41
 network 100.2.1.0 0.0.0.3 area 0
 network 100.2.0.1 0.0.0.0 area 0
 passive-interface default
 no passive-interface serial 0/0
 log-adjacency-changes
```

    Note: From release 12.1 onwards, the "ospf" directive should be omitted when enabling "log-adjacency-changes".

22. **DMZ between AS10 and AS20.** OSPF must **NOT** run on the demarcation links between AS10 and AS20. So Routers 6, 7, 8 and 9 must **NOT** configure the serial links between each other to be non-passive. This is a very important point, and a mistake frequently made by many ISPs. Router 6

should have two adjacencies only – with Router 4 and 5. Router 7 should have one adjacency only – with Router 9. And so on.

23. **Intra Area Authentication – Part 1.** OSPF supports router authentication within areas. This is very important inside ISP networks to prevent the introduction of improperly configured or unintended equipment.

    This first step will enable authentication for the OSPF area the router is in. To do this, the *area N authentication message-digest* command is used. An example configuration might be:

```
router ospf 41
 area 0 authentication message-digest
!
```

    Note that this does not affect the actual adjacencies on the routers – it only tells the router that the area mentioned will use authentication, if it is configured.

24. **Intra Area Authentication – Part 2**. Now that support for authentication in the area has been configured, the second step is to actually set the authentication password to be used, and the interface it has to be used on. The password that should be used for all areas in this example is *cisco*. MD5 encryption should be used rather than the standard simple encryption – to do this, use the *message-digest-key* sub-interface command.

    An example configuration might be:

```
router ospf 41
 area 0 authentication message-digest
!
interface ethernet 0/0
 ip ospf message-digest-key 1 md5 cisco
interface serial 0/0
 ip ospf message-digest-key 1 md5 cisco
interface serial 0/1
 ip ospf message-digest-key 1 md5 cisco
!
```

    Notice now that the OSPF adjacencies do not come up unless the neighbouring router has also entered the same configuration and key. Notice also how the OSPF adjacencies were reset as the configuration was entered – security is being introduced, so the adjacencies are reset.

    Note: the *message-digest-key* allows up to 255 keys to be set per interface. It is generally not recommended to set more than one per interface, as the router will try and communicate with its neighbours using all keys. If a key needs to be upgraded, common practice then is to set a second key, allowing a graceful changeover without compromising the functioning of the network. Once all the routers on the network are using the new key, the old one should be removed.

25. **Ping Test #2.** Ping all loopback interfaces in your AS. They should all respond. This will ensure the OSPF IGP is connected End-to-End. If there are problems, use the following commands to help determine the problem:

```
show ip route          : see if there is a route for the intended destination
show ip ospf           : see general OSPF information
```

```
show ip ospf interface      : Check if OSPF is enabled on all intended interface
show ip ospf neighbor       : see a list of OSPF neighbours that the router sees
```

Checkpoint #2: *call lab assistant to verify the connectivity. Save the configuration as it is on the router either on the worksheet on the end of this hand out, or own your own laptop, or on the classroom tftp server if it is available.*

26. BGP distance. Before we set up iBGP with our neighbours in our AS, we need to do some basic preparation on the router. The IOS defaults are not optimised for Service Provider networks, so before we bring up BGP sessions, we should set the defaults that we require.

The default distance for eBGP is 20, the default distance for iBGP is 200, and the default distance for OSPF is 110. This means that there is a potential for a prefix learned by eBGP to override the identical prefix carried by OSPF. Recall from the Routing presentation that there is a distinct separation between BGP and OSPF processes – prefixes present in OSPF will never be found in BGP, and vice-versa. To protect against accidents[2], the eBGP distance is set to 200 also. The command to do this is the bgp distance subcommand, syntax is:

```
distance bgp <external-routes> <internal-routes> <local-routes>
```

Note: This should be included in all future BGP configurations in this workshop. Set the BGP protocol distance so that BGP is always less preferred than any IGP. So:

```
router bgp 10
 distance bgp 200 200 200
```

27. Passwords on BGP sessions. It is now considered very good practice to use passwords on the BGP sessions on the router. When BGP is set up in the next step, don't forget to include a password on the BGP peering.

The password used for this module will be *cisco* – obviously on a real operational network operators will use a password which follows their normal password rules, and not something which is easily guessable. An example configuration might be:

```
router bgp 10
 neighbor 1.2.3.4 password cisco
```

Note: Passwords should be included in all future BGP configurations in this workshop.

28. Configuring iBGP Neighbours. Configure iBGP peers within each autonomous system. Use a full iBGP mesh. Don't forget that iBGP peering is configured to be between the loopback interfaces on the routers. Also, it is good practice to use a peer-group. For example:

```
router bgp 10
 neighbor ibgp-peers peer-group
 neighbor ibgp-peers remote-as 10
 neighbor ibgp-peers description iBGP peergroup for internal routers
```

[2] There have been several incidents in the past where denial of service attacks on ISP networks have been successful because ISPs have omitted basic routing protocol security. Setting the BGP distances to be greater than any IGP is one of the mitigation methods available.

```
 neighbor ibgp-peers update-source loopback 0
 neighbor ibgp-peers password cisco
 neighbor ibgp-peers send-community
 neighbor 100.2.0.1 peer-group ibgp-peers
 neighbor 100.2.0.2 peer-group ibgp-peers
 neighbor 100.2.0.3 peer-group ibgp-peers
..etc..
```

Use *show ip bgp summary* to check the status of the iBGP neighbour connections. If the iBGP session is not up and/or no updates are being sent, work with the Router Team for that neighbour connection to troubleshoot the problem. Note: get into the habit of using peer-groups and configuring them fully, including the "send-community" directive. This workshop makes extensive use of communities, and making them part of your configuration is good practice.

Note: Router6 should also include the network connecting to Router15 in the iBGP configuration. This is so that the network connected to Router15 can be accessed – it has the DNS server and NTP server located on it.

29. **Add Prefixes to BGP.** Each Router Team will advertise the CIDR block assigned to them via BGP. AS10 would advertise 100.1.0.0/19 and AS20 would advertise 100.2.0.0/19:

```
router bgp 10
 no synchronization
 no auto-summary
 bgp log-neighbor-changes
 network 100.2.0.0 mask 255.255.224.0
!
ip route 100.2.0.0 255.255.224.0 null0
```

Don't forget the static route to Null0. This ensures that the prefix has an entry in the routing table, and therefore will appear in the BGP table. Also, don't forget to disable synchronisation and auto-summarisation – these are also mandatory requirements for ISP routers connecting to the Internet. (Note that a distance of 250 could be applied to the static route to ensure that routing protocols announcing this exact prefix will override the static (if this is required/desired).)

Checkpoint #3: *call the lab assistant to verify the connectivity.*

30. **Enable new format of BGP communities.** It is also worth getting into the habit of changing the BGP community format from the default 32-bit integer to colon separated 16-bit integers, as used in RFC1998. Example:

```
ip bgp-community new-format
```

31. **Configure eBGP peering.** Now that iBGP is functioning, it is time to configure eBGP. External BGP will be set up between AS10 and AS20, specifically between Routers 6 and 8, and Routers 7 and 9 only. The remaining lab teams should monitor the BGP table they see on their routers.

Firstly, agree on what IP addresses should be used for the point to point links between the ASes. Put the /30 networks used for the DMZ links into OSPF (network statement and passive interface). Then configure eBGP between the router pairs, for example:

```
router bgp 10
 neighbor 100.2.2.2 remote-as 20
 neighbor 100.2.2.2 password cisco
 neighbor 100.2.2.2 description eBGP with RouterXX
```

Use the BGP show commands to ensure that you are receiving prefixes from your neighbouring AS.

32. **Check the network paths and the routing table.** Run traceroutes between your router and other routers in the classroom. Ensure that all routers are reachable. If any are not, work with the other router teams to establish what might be wrong. Make sure that you can see Router15. The lab instructor will have written the addresses and network up on the whiteboard. (The network is 192.168.1.0/24, the address of Router6 on that LAN is 192.168.1.254, and the address of Router15 is 192.168.1.1.)

33. **Saving the configuration. For software releases from 12.0 onwards**, the commands to save the configuration are of the format *copy <source> <destination>* where the source and destinations can be any of the following options: *ftp, lex, null, nvram, rcp, running-config, startup-config, system, tftp.* To save the configuration to the TFTP server, use the "*copy system:/running-config tftp:"* command sequence. If the TFTP server is unreachable, "."s followed by an error message will be displayed rather than "!"s. (Note that the "*write net*" command of earlier releases is still supported but may be removed at a future release.)

    An example of saving the configuration for Router 1 might be:

```
Router1#copy system:/running-config tftp:
Address or name of remote host[]? 192.168.1.4
Destination filename [running-config]? router1-confg
!!
2259 bytes copied in 2.920 secs (1129 bytes/sec)
Router1#
```

Checkpoint #4: *call the lab assistant to verify the connectivity.*

34. **Summary.** This module has covered most of the fundamental configuration topics required to construct an ISP network. It has covered basic router configuration, configuration Best Current Practices, OSPF configuration, iBGP configuration, and finally simple eBGP configuration. No routing policy has been implemented. **Each Router team is strongly recommended to make a copy of their configuration as most of the configuration concepts will be required throughout the remainder of the workshop.**

Cisco Systems Inc
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

CONFIGURATION NOTES

Documentation is critical! You should record the configuration at each ***Checkpoint***, as well as the configuration at the end of the module.