IPv6 Security Lab

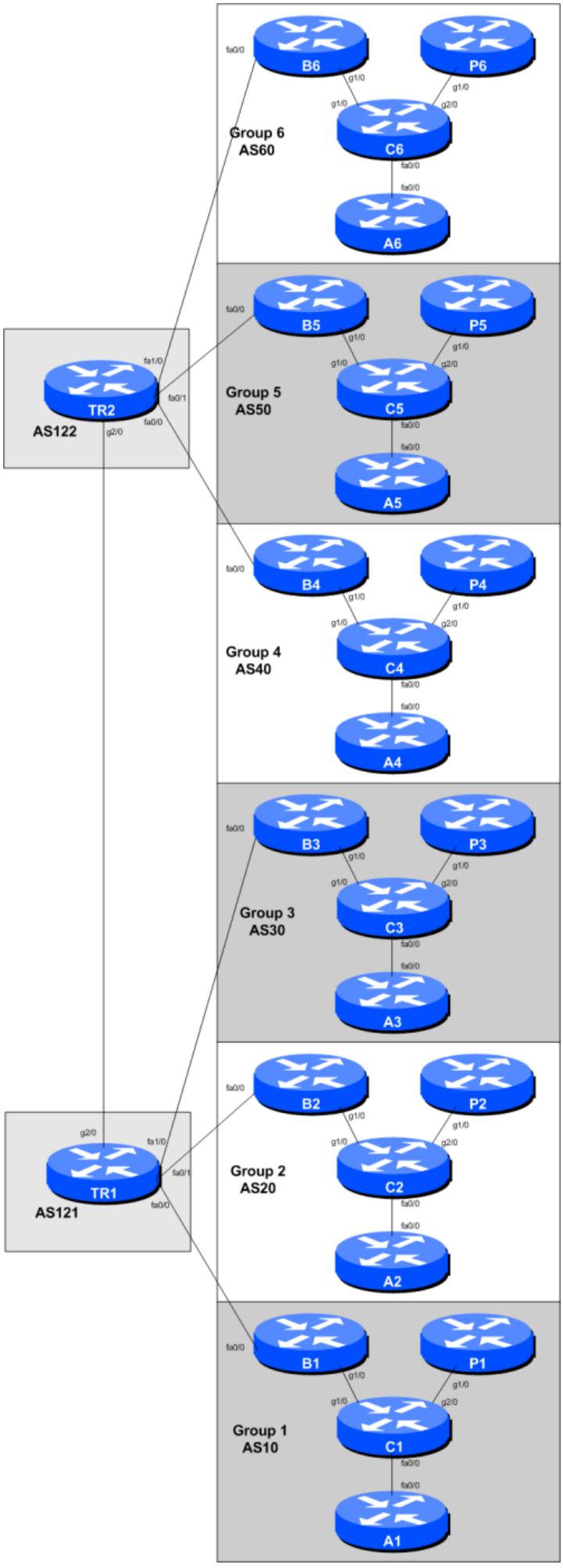
Objective

Using a dual stack topology, this lab investigates securing the router and the routing infrastructure for the network.

Lab Topology

The initial lab topology sets up 6 autonomous systems, each with four routers. In each AS, one router is the border router (for connecting to transit providers), one router is the core router (representing the rest of the network operator's core network), one router is a peering router (for connecting to private peers and IXPs), and one router is an access router (nominally where end users connect to the network).

The lab will start simply by configuring each autonomous system, and making sure that transit works via their transit provider. The address plan for the entire network is described in the [Address Plan](address-plan) document. The initial set up is shown below.


Group 6
AS60
B6
P6
C6
A6
Group 5
AS50
B5
P5
C5
A5
Group 4
AS40
B4
P4
C4
A4
Group 3
AS30
B3
P3
C3
A3
Group 2
AS20
B2
P2
C2
A2
Group 1
AS10
B1
P1
C1
A1
AS122
TR2
AS121
TR1
fa0/0
g1/0
g2/0
fa1/0
fa0/1

Preliminary

Introducing the lab

This workshop uses Cisco IOS routers running IOS, but on the Dynamips systems – Dynamips translates the Cisco 7200 router processor instructions in IOS to those of the Intel based host system, allowing Cisco IOS images, and therefore network configurations, to be run on a host PC system (usual Linux or MacOS based).

The lab will have been preconfigured by the instructors, allowing participants to enter the following exercises directly. Please read the following steps carefully.

Accessing the lab

Each participant will be assigned to a group. Depending on the number of participants, either a single person or a group will be responsible for the configuration of a router. You may be asked to rotate and work on a different router so that you have the opportunity to understand the network from another point of view.

As you go through the exercises, you will see examples of configurations for one or more routers. **Make sure to take those examples and adapt them to your own router, network topology and addressing scheme. Use the diagrams to guide you.**

Refer to the [Lab Access Instructions](lab-access) document for information about logging into the routers that have been assigned to you.

Basic Router Configuration

The following configuration examples show the suggested/recommended configuration to be implemented on the routers in each group. Replace the **RX** in the examples with the router type (either B for Border or C for Core or P for Peering or A for Access) and Group number as appropriate.

The following configuration examples show the suggested/recommended configuration to be implemented on the routers in each group. Replace the **RX** in the examples with the router type (either B for Border or C for Core or P for Peering or A for Access) and Group number as appropriate.

Name the router

```
Router> enable
Router# config terminal
Router(config)# hostname RX
```

Configure Authentication

```
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
username seclab secret lab-PW
enable secret lab-EN
service password-encryption
line vty 0 4
 transport preferred none
line console 0
 transport preferred none
```

Configure logging

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

Disable DNS resolution

```
no ip domain-lookup
```

Activate IPv6 routing

Turn on IPv6 Routing and activate IPv6 CEF (not on by default in Cisco IOS)

```
ipv6 unicast-routing
ipv6 cef
```

Disable source routing for IPv4 and IPv6

```
no ip source-route
no ipv6 source-route
```

Path MTU Discovery

Enable Path MTU Discovery on the router - this is not enabled by default for connections to the control plane (but it is enabled by default now for BGP).

```
ip tcp path-mtu-discovery
```

Exit configuration mode and save

```
end
write memory
```

Summary of the commands entered

Turn Off Domain Name Lookups

Cisco routers will always try to look up the DNS for any name or address specified in the command line.

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.

Enable IPv6

Cisco routers with an IOS supporting IPv6 currently do not ship with IPv6 enabled by default.

Enable IPv6 CEF

Unlike IPv4, CEFv6 is not enabled by default.

Disable IPv4 and IPv6 Source Routing

Unless you really believe there is a need for it, source routing should be disabled. This option, enabled by default, allows the router to process packets with source routing header options. This feature is a well-known security risk.

Usernames and Passwords

All router usernames should be **seclab** and password should be **lab-PW**. Configuration mode password should be **lab-EN**.

service password-encryption

This directive tells the router to encrypt all passwords stored in the router’s configuration (apart from *enable secret* which is already encrypted).

Enabling login access for other teams

This is done using the **aaa new-model** directive in IOS.

Configure system logging

A vital part of any Internet operational system is to record logs. We disables console logs and instead record all logs in a 8192 byte buffer set aside on the router.

Interface Configuration

Loopback

First we will configure the Loopback interface of each of the routers.

On CX:

```
interface Loopback0
 description Loopback of CX
 ip address 100.68.X0.2 255.255.255.255
 ipv6 address 2001:db8:X0::2/128
```

You will need a similar configuration for the Peering, Access and Border router as well.

Links to other Routers

Now we will configure the router physical interfaces according to the diagram.

The configuration example below shows what to do for the link between CX and BX. You will need to set up similar configuration for the links between CX and AX and between CX and PX.

On CX:

```
interface GigabitEthernet1/0
 description P2P Link to BX
 ip address 100.68.X0.17 255.255.255.252
 no ip directed-broadcast
 no ip redirects
 no ip proxy-arp
 ipv6 address 2001:db8:X0:10::0/127
 ipv6 nd prefix default no-advertise
 ipv6 nd ra suppress all
 no shutdown
!
```

On BX:

```
interface GigabitEthernet1/0
 description P2P Link to CX
 ip address 100.68.X0.18 255.255.255.252
 no ip directed-broadcast
```

```
 no ip redirects
 no ip proxy-arp
 ipv6 address 2001:db8:X0:10::1/127
 ipv6 nd prefix default no-advertise
 ipv6 nd ra suppress all
 no shutdown
!
```

Explanations for some of the commands used

no ip directed-broadcast

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend disabling the *ip directed-broadcast* command on any intereface where directed broadcasts are not needed (probably all).

no ip proxy-arp

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By “faking” its identity, the router accepts responsibility for routing packets to the “real” destination. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.

Disadvantages of proxy arp:

- It increases the impact of ARP spoofing, in which a machine claims to be another in order to intercept packets.

- It hides network misconfigurations in hosts

- Hosts will have larger ARP tables

no ip redirects

ICMP redirects can be sent to a host when the router knows that another router in the same subnet has a better path to a destination. If a hacker installs a router in the network that causes the legitimate router to learn these ilegitimate paths, the hacker's router will end up diverting legitimate traffic thanks to ICMP redirects. Thus, we recommend that you disable this feature in all your interfaces.

ipv6 nd ra suppress

IPv6 router advertisements are sent periodically by routers to inform hosts that the router is present,

and to allow hosts to autoconfigure themselves using stateless autoconfiguration mechanisms. This is not necessary on point-to-point interfaces.

ipv6 nd prefix default no-advertise

This prevents the router from sending any prefixes as part of router advertisements, so the client will not auto-configure itself with a global IPv6 address. This is helpful for IOS versions where you cannot suppress solicited RA messages.

Connectivity Testing

Do some PING tests

```
C1# ping 100.68.10.18       <- B1
C1# ping 2001:DB8:10:10::1  <- B1
C1# ping 100.68.10.22       <- P1
C1# ping 2001:DB8:10:11::1  <- P1
```

and then verify the output of the following commands:

```
show arp              : Show ARP cache
show interface        : Show interface state and config
show ip interface     : Show interface IP state and config
show ipv6 neighbors   : Show IPv6 neighbours
show ipv6 interface   : Show interface state and config
show cdp neighbors    : Show neighbours seen via CDP
```

Save Configuration

Verify and save the configuration.

```
show running-config
write memory
```

From:
https://www.bgp4all.com/pfs/ - **Philip Smith's Internet Development Site**

Permanent link:
https://www.bgp4all.com/pfs/training/pacnog21/0-setup?rev=1508283560

Last update: **2017/10/17 23:39**