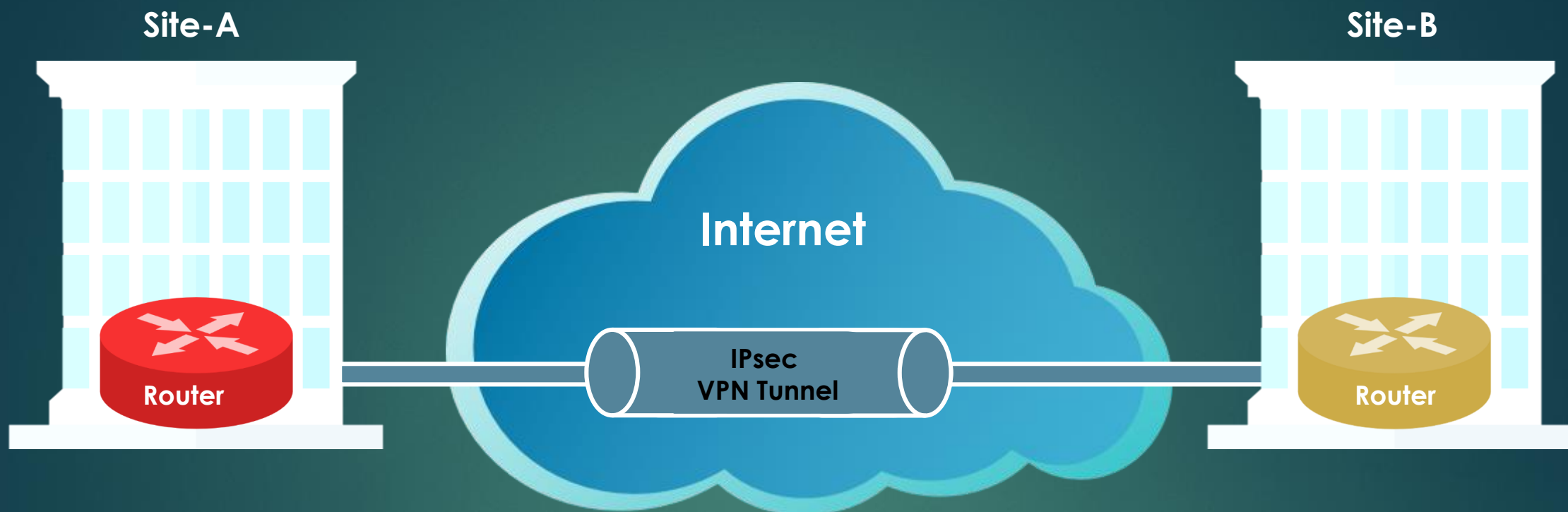
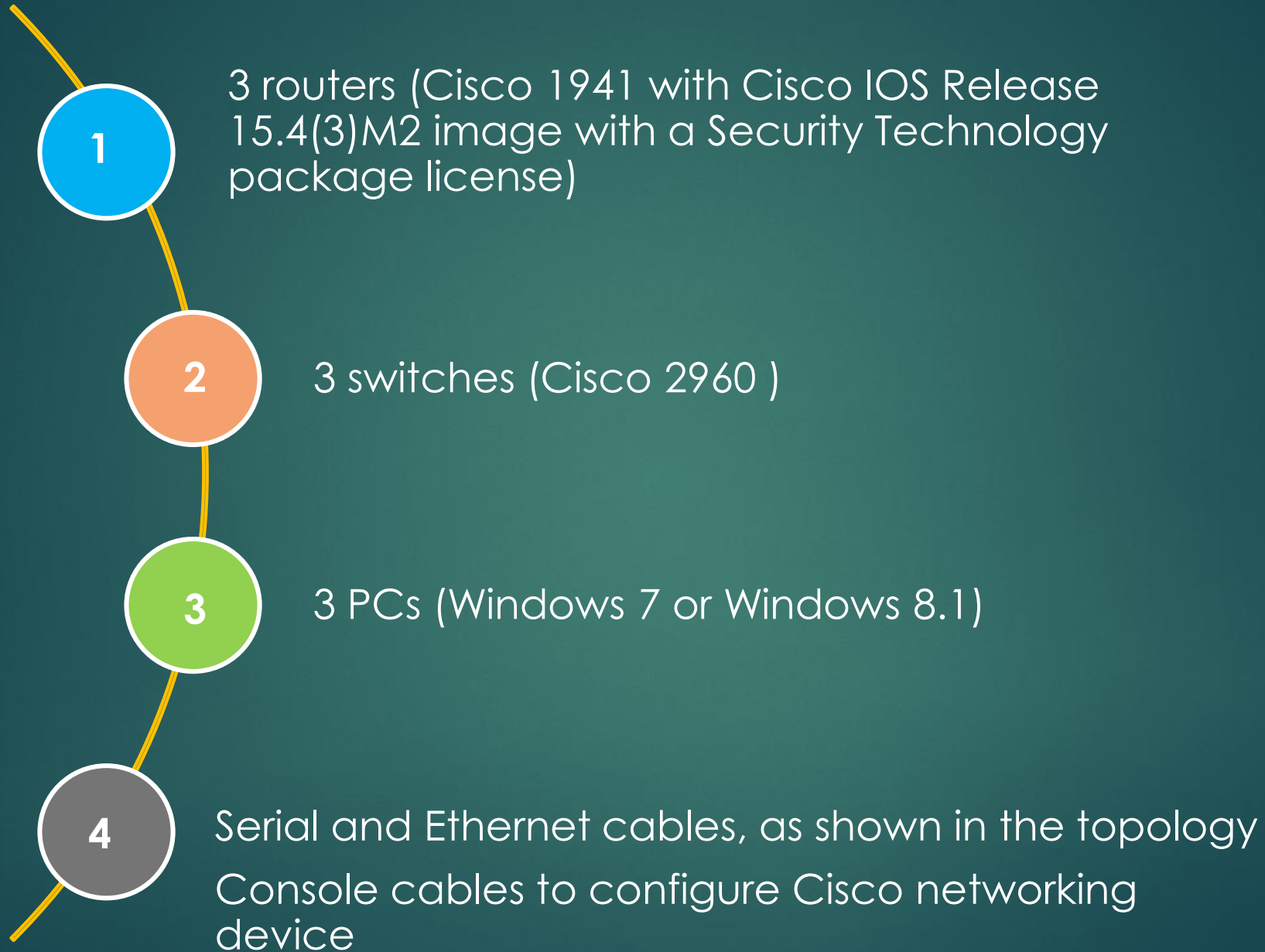




Site to Site IPsec VPN Using CLI

*By Eng. Ala'aldin Sweilem
Network Engineer
Alaswelm2013@gmail.com*

Required Resources



This lab implemented by packet tracer 7.2.1



The banner features a dark blue background with green circuit-like lines. At the top left is the Cisco Academy logo. At the top right is a blue brain icon connected to a green plug. At the bottom right is a yellow lightbulb icon with a green base. A horizontal strip of six images is in the center, each with a corresponding colored label below it: 'Courses in 20+ Languages' (blue), 'Hands-On' (teal), 'Flexible Delivery' (light blue), 'Supports Personalized Instruction' (green), 'Simulations' (orange), and 'Hackathons' (red).

Networking
CISCO Academy

Cisco Packet Tracer

An innovative and powerful networking simulation tool used for practice, discovery and troubleshooting

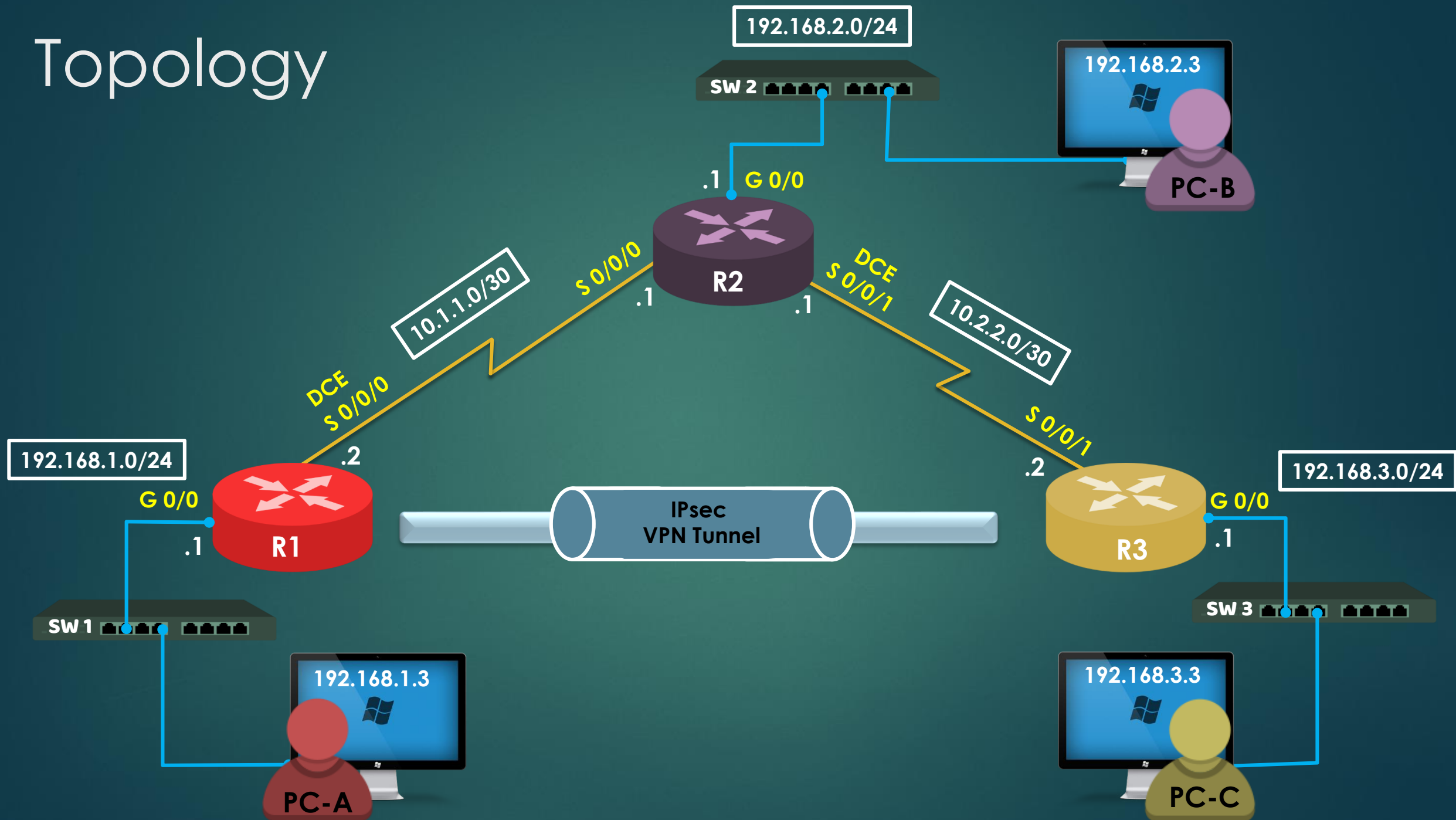
Courses in 20+ Languages | Hands-On | Flexible Delivery | Supports Personalized Instruction | Simulations | Hackathons

Integral to the Skills-to-Jobs Learning Experience

© Copyright Cisco 2018

Version: 7.2.1.0218
[Copyright Cisco 2018 EULA](#)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
	G 0/0	192.168.1.1	255.255.255.0	...
	S 0/0/0 (DCE)	10.1.1.2	255.255.255.252	...
	G 0/0	192.168.2.1	255.255.255.0	...
	S 0/0/0	10.1.1.1	255.255.255.252	...
	S 0/0/1 (DCE)	10.2.2.1	255.255.255.252	...
	G 0/0	192.168.3.1	255.255.255.0	...
	S 0/0/1	10.2.2.2	255.255.255.252	...
 PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
 PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
 PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Configure Basic Device Settings

- A. Configure interface IP addresses for each router
- B. Configure the OSPF dynamic routing protocol
- C. Configure PC host IP settings
- D. Verify basic network connectivity

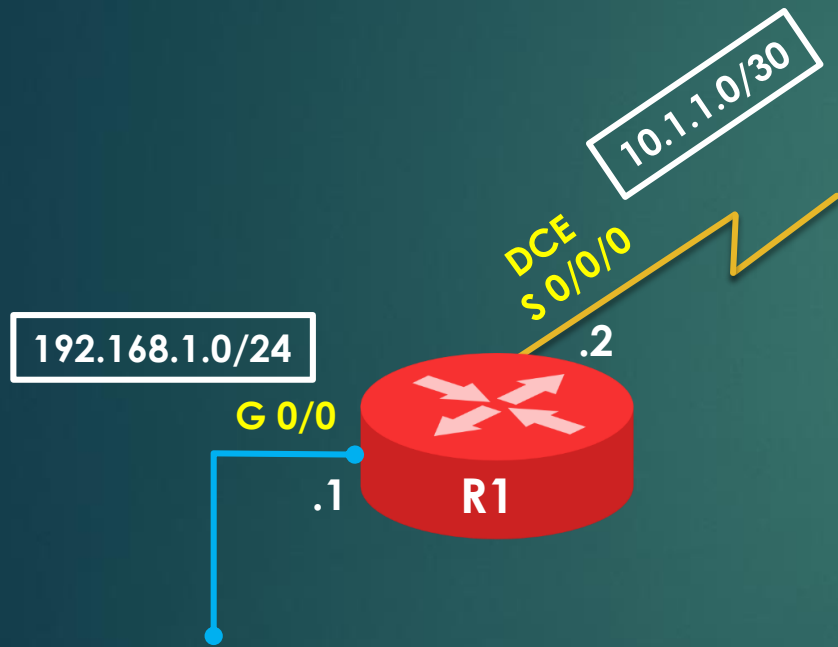
Part 2: Configure a Site-to-Site VPN Using Cisco IOS

- A. Planning and Preparing an IPsec Site-to-Site VPN
- B. Configure IPsec VPN settings on R1 and R3
- C. Verify IPsec VPN operation

Part 1-A

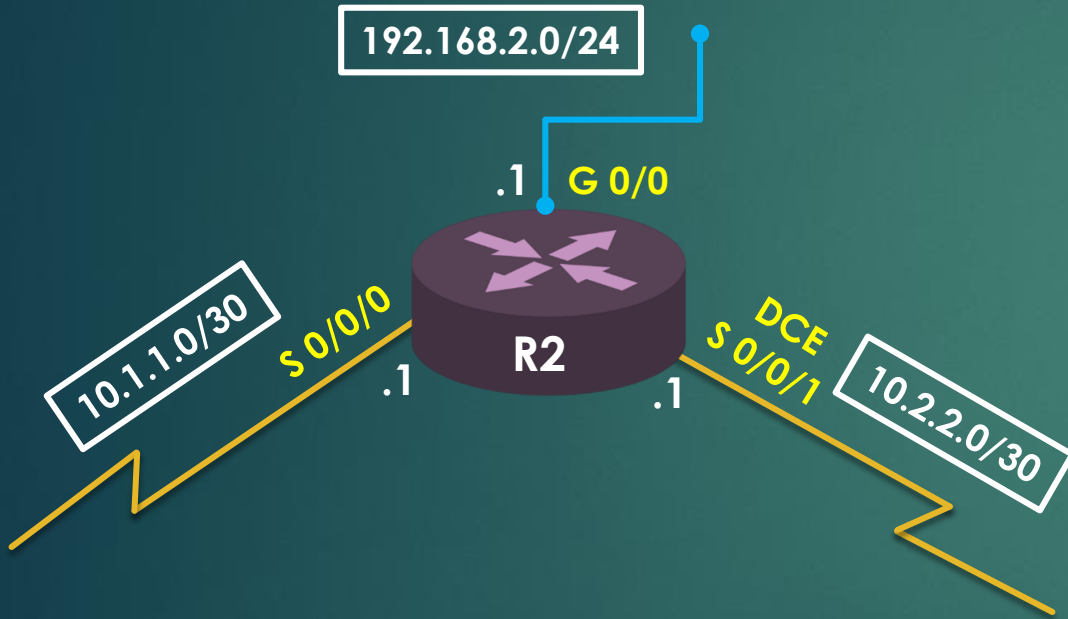
Configure interface IP addresses

Configure interface IP addresses for the R1



- ▶ Config t
- ▶ Int G 0/0
- ▶ ip add 192.168.1.1 255.255.255.0
- ▶ no shut
- ▶ int S 0/0/0
- ▶ clock rate 64000
- ▶ ip add 10.1.1.2 255.255.255.252
- ▶ no shut

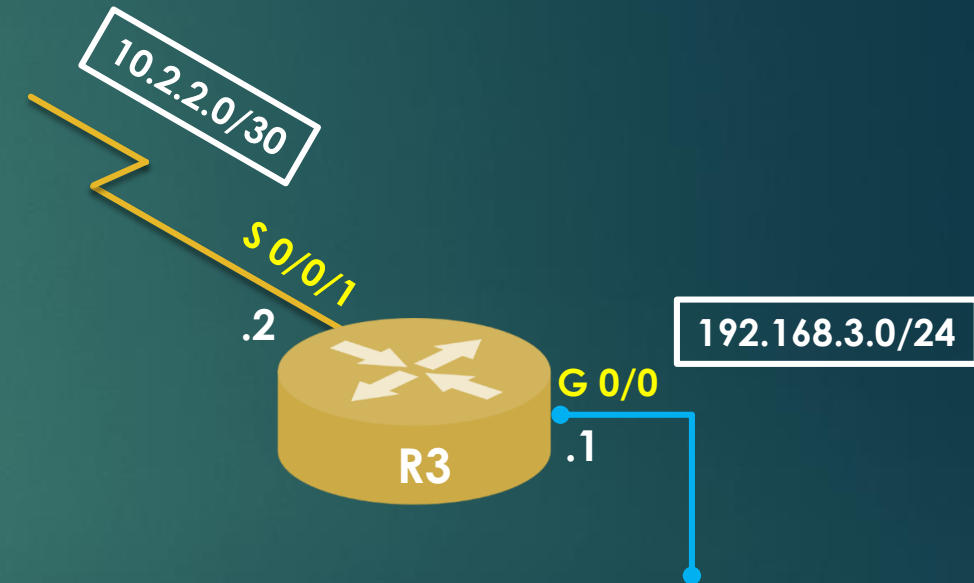
Configure interface IP addresses for the R2



- ▶ Config t
- ▶ Int G 0/0
- ▶ ip add 192.168.2.1 255.255.255.0
- ▶ no shut
- ▶ int S 0/0/0
- ▶ ip add 10.1.1.1 255.255.255.252
- ▶ no shut
- ▶ int S 0/0/1
- ▶ clock rate 64000
- ▶ ip add 10.2.2.1 255.255.255.252
- ▶ no shut

Configure interface IP addresses for the R3

- ▶ Config t
- ▶ Int G 0/0
- ▶ ip add 192.168.3.1 255.255.255.0
- ▶ no shut
-
- ▶ int S 0/0/1
- ▶ ip add 10.2.2.2 255.255.255.252
- ▶ no shut



Part 1-B

Configure the OSPF dynamic routing protocol



R1

On R1, use the following commands:

- ▶ R1(config)# router ospf 101
- ▶ R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
- ▶ R1(config-router)# network 10.1.1.0 0.0.0.3 area 0



R2

On R2, use the following commands:

- ▶ R2(config)# router ospf 101
- ▶ R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
- ▶ R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
- ▶ R2(config-router)# network 192.168.2.0 0.0.0.255 area 0



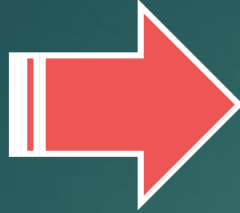
R3

On R3, use the following commands:

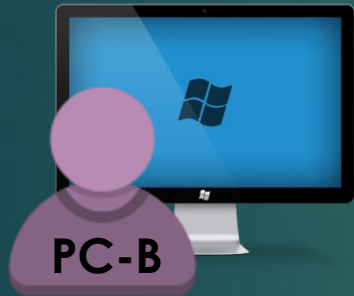
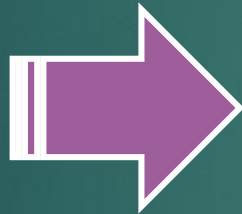
- ▶ R3(config)# router ospf 101
- ▶ R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
- ▶ R3(config-router)# network 10.2.2.0 0.0.0.3 area 0

Part 1-C

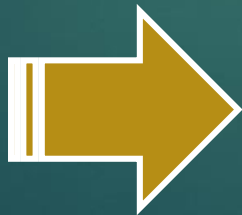
Configure PC host IP settings



- ▶ IP : 192.168.1.3
- ▶ SM : 255.255.255.0
- ▶ DG : 192.168.1.1



- ▶ IP : 192.168.2.3
- ▶ SM : 255.255.255.0
- ▶ DG : 192.168.2.1



- ▶ IP : 192.168.3.3
- ▶ SM : 255.255.255.0
- ▶ DG : 192.168.3.1

Part 1-D

Verify basic network connectivity

1



R1# ping 192.168.3.1



- ▶ Ping from R1 to the R3 G 0/0 interface at IP address 192.168.3.1.
- ▶ If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

2



PC-A:\> ping 192.168.3.3



- ▶ Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.
- ▶ If the pings are unsuccessful, troubleshoot the basic device configurations before continuing

Part 2-A

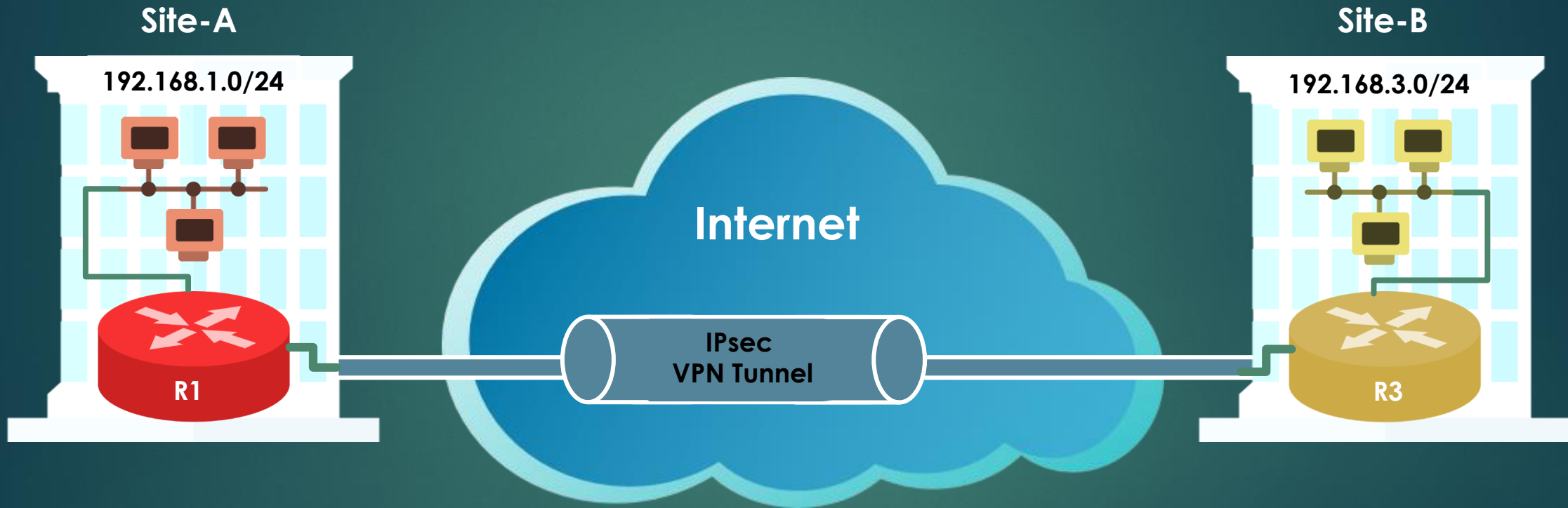
Planning and Preparing an IPsec Site-to-Site VPN

Planning and Preparing IPsec VPN

- 1 Identify a customer's needs for VPN services
- 2 Ensure that all ACLs in the IPsec VPN network path are compatible with IPsec
- 3 Planning IKEv1 Phase 1 (ISAKMP SA policy)
- 4 Planning IKEv1 Phase 2 (IPsec SA policy)

1

Identify a customer's needs for VPN services and plan out the details to implement the VPN

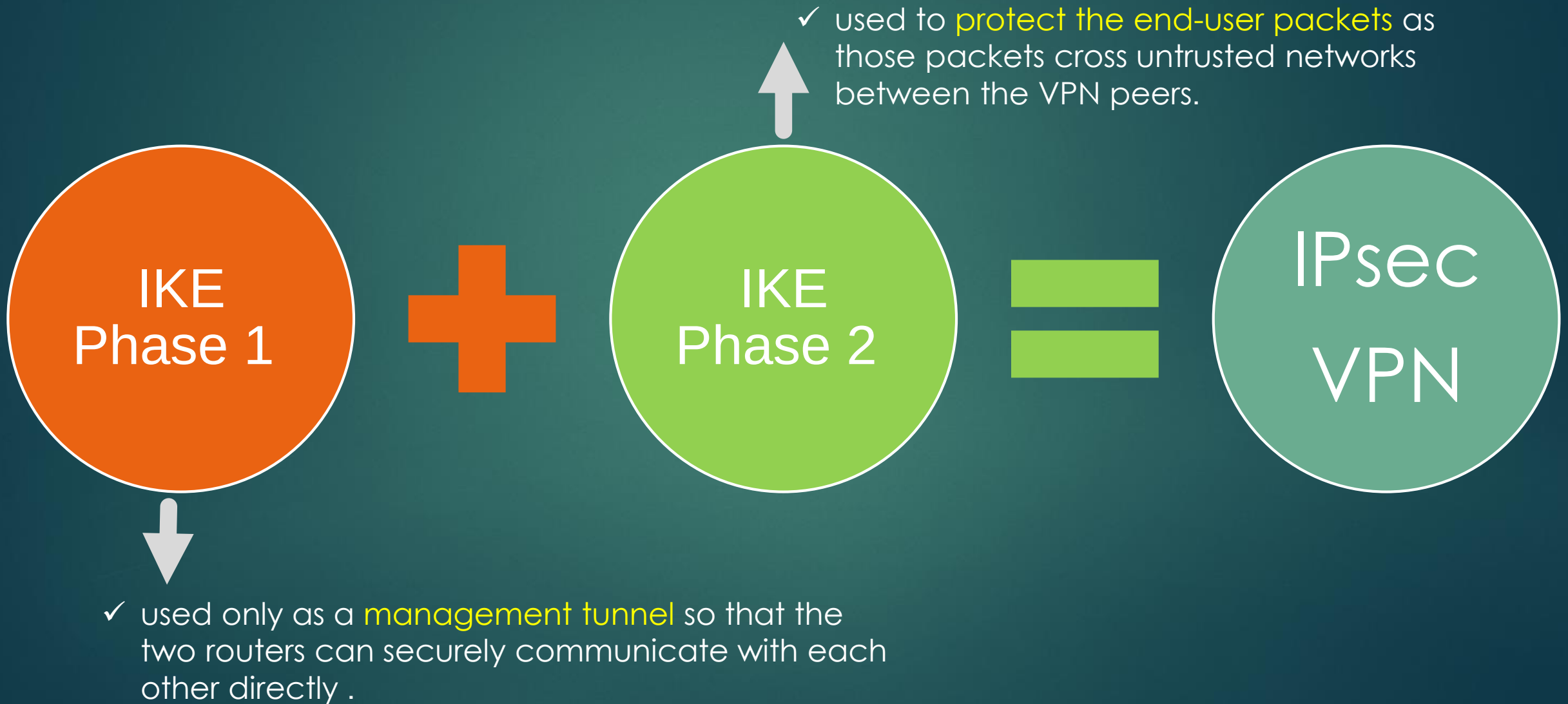


- ✓ The customer has asked us for a recommendation to allow file services between the two offices that can be done **securely**.
- ✓ The customer also wants to ensure that the data as it is being sent over the networks does **not become altered or corrupted in transit**

2 Ensure that all ACLs in the IPsec VPN network path are compatible with IPsec

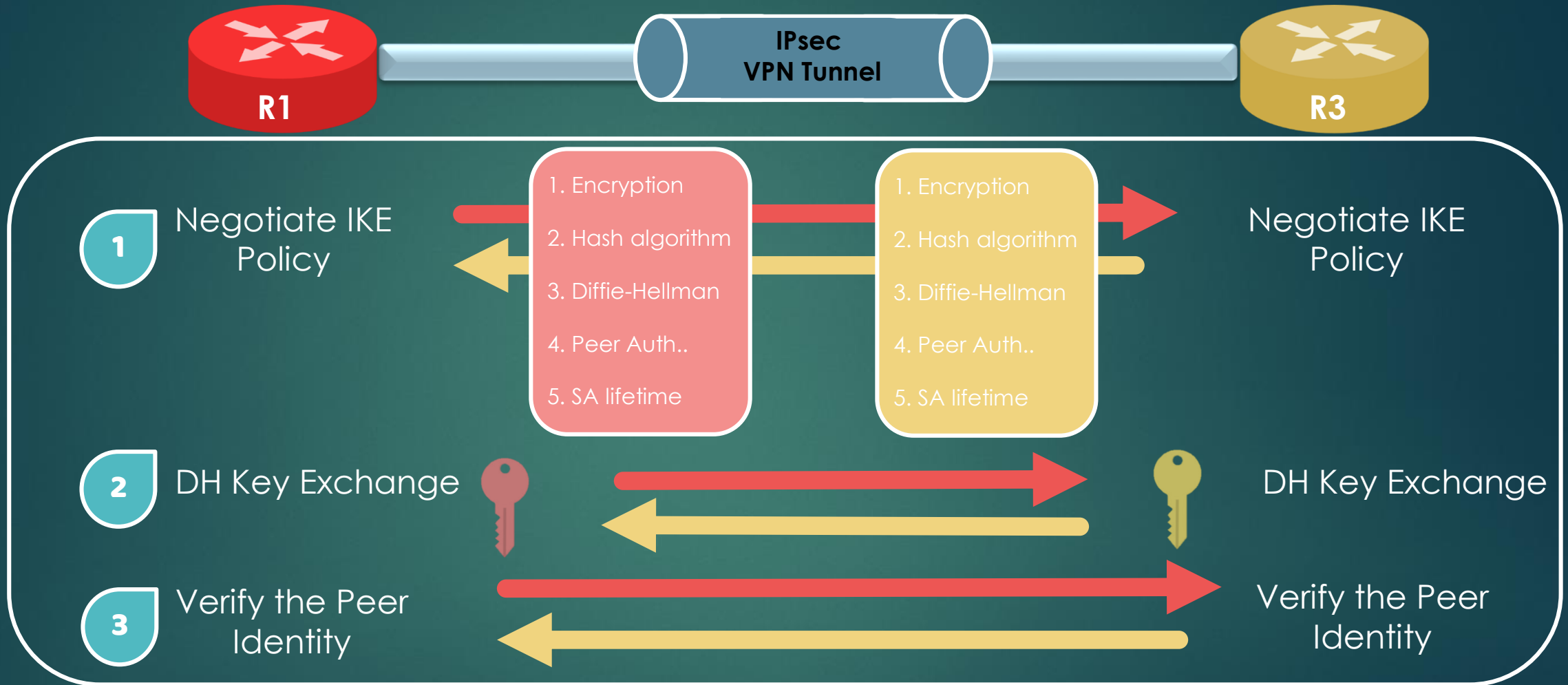
- ▶ The first step in configuring Cisco IOS ISAKMP is to ensure that existing ACLs on perimeter routers, firewalls, or other devices do not block IPsec traffic.
- ▶ permit protocol 50 (ESP), protocol 51 (AH), and UDP port 500 (ISAKMP) traffic. They also would permit UDP port 4500 (non500-isakmp). This is used by NAT-T, which is a commonly implemented extension to IKE and has been incorporated into IKEv2. NAT-T facilitates VPN through intermediate devices that perform Port Address Translation (PAT).

There are two phases in every IKE negotiation



Phase 1 and 2 Key Negotiation

Phase 1



Phase 2



3

ISAKMP Phase 1 Policy Parameters

✓ Note: Bolded parameters are defaults Only unbolded parameters have to be explicitly configured

Parameters	 R1	 R3
Key Distribution Method Manual or ISAKMP	ISAKMP	ISAKMP
Encryption Algorithm DES , 3DES, or AES	AES 256	AES 256
Hash Algorithm MD5 or SHA-1	SHA-1	SHA-1
Authentication Method Pre-shared keys or RSA	pre-share	pre-share
Group # for DH key exchange DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime 86400 seconds or less	86400	86400
ISAKMP Key	cisco123	cisco123

4

IPsec Phase 2 Policy Parameters

Parameters	 R1	 R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Part 2-B

Configure IPsec VPN settings on R1 and R3

Configure IPsec VPN settings on R1



1

Enable the Security Technology package

2

Identify interesting traffic on Router

3

Configure the IKE Phase 1 ISAKMP policy

4

Configure the IKE Phase 2 IPsec policy

5

Configure the crypto map

1

Enable the Security Technology package

- ▶ On R1, issue the **show version command** to view the Security Technology package license information.
- ▶ If the Security Technology package has not been enabled, use the following command to enable the package.
- ▶ R1(config)# **license boot module c1900 technology-package securityk9**
- ▶ Accept the end-user license agreement.(**type yes**)
- ▶ **Save the running-config**
- ▶ **reload** the router to enable the security license.
- ▶ **Verify** that the Security Technology package has been enabled by using the **show version command**

view the Security Technology package

► show version

```
License Info:

License UDI:

-----
Device#      PID                      SN
-----
*0           CISCO1941/K9              FTX1524C38B-

Technology Package License Information for Module:'c1900'

-----
Technology    Technology-package      Technology-package
              Current        Type                Next reboot
-----
ipbase        ipbasek9               Permanent          ipbasek9
security      securityk9              Evaluation          securityk9
data          disable                 None                None

Configuration register is 0x2102

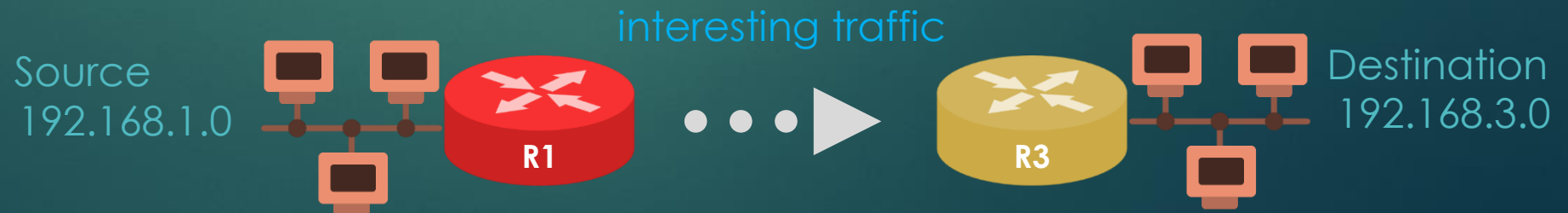
Router>
```



2

Identify interesting traffic on R1.

- ▶ Configure **ACL 110** to identify the traffic from the LAN on R1 to the LAN on R3 **as interesting**.
- ▶ This interesting traffic will trigger the **IPsec VPN** to be implemented when there is traffic between the R1 to R3 LANs.
- ▶ All other traffic sourced from the LANs will not be encrypted. Because of the implicit deny all, there is no need to configure a deny ip any statement.
- ▶ R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**



3

Configure the IKE Phase 1 ISAKMP policy

- ▶ Configure the **crypto ISAKMP policy 10** properties on R1 along with the shared crypto key **cisco123**.
- ▶ Refer to the **ISAKMP Phase 1 table** for the specific parameters to configure. **Default values do not have to be configured**. Therefore, only the encryption method, key exchange method, and DH method must be configured.
- ▶ Note: The highest DH group currently supported by Packet Tracer is **group 5**.
In a production network, you would configure at least DH 14.

```
R1(config)# crypto isakmp policy 10
```

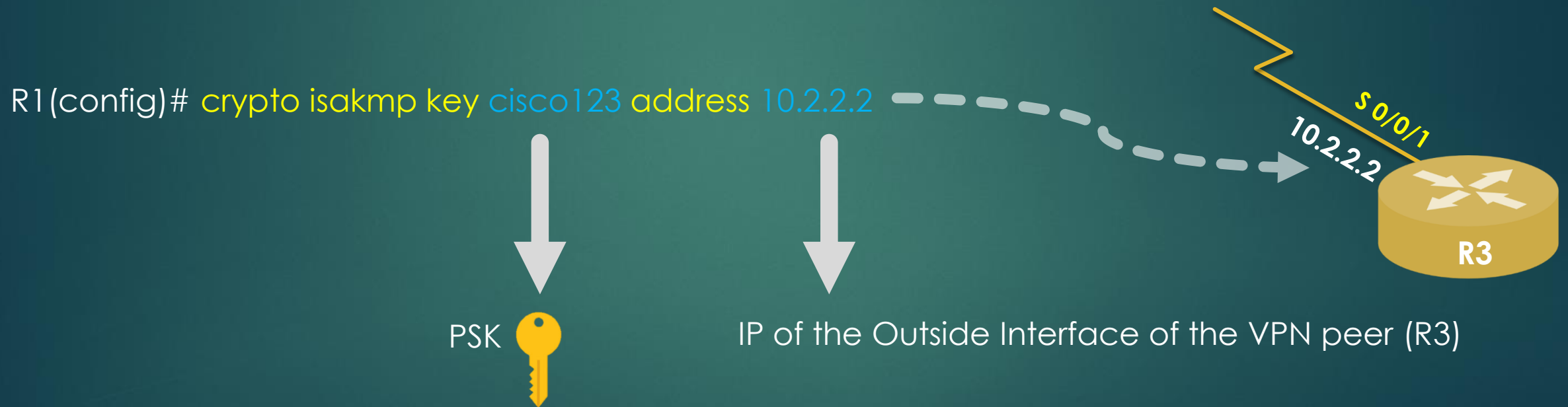
```
R1(config-isakmp)# encryption aes 256
```

```
R1(config-isakmp)# authentication pre-share
```

```
R1(config-isakmp)# group 5
```

Configure the pre-shared key (PSK)

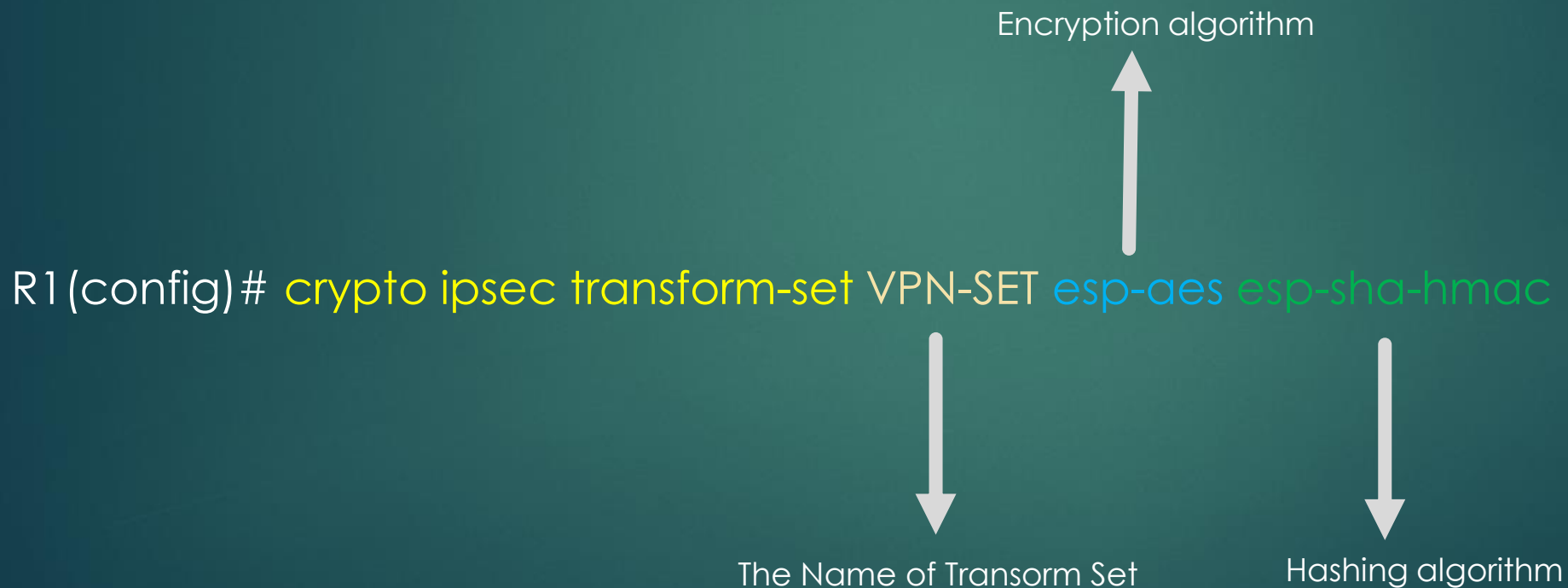
- ▶ The PSK allow the VPN peers to authentication each other



4

Configure the IKE Phase 2 IPsec policy

- The set of encryption and hashing algorithm that will be used to transform data sent through the IPsec Tunnel. This is called the transform set.



5

Configure the **crypto map**

- Create the **crypto map VPN-MAP** that binds all of the **Phase 2 parameters** together. Use sequence number 10 and identify it as an ipsec-isakmp map.

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
```

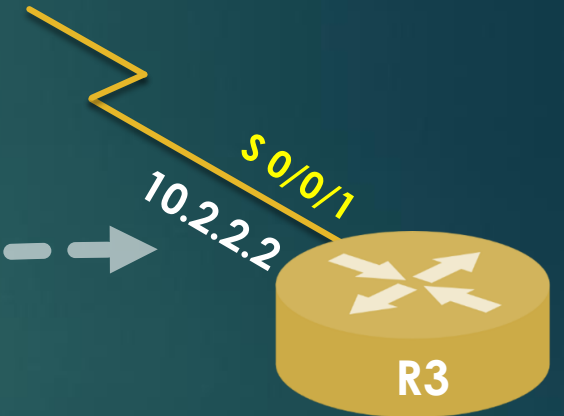
```
R1(config-crypto-map)# description VPN connection to R3
```

```
R1(config-crypto-map)# set peer 10.2.2.2
```

```
R1(config-crypto-map)# set transform-set VPN-SET
```

```
R1(config-crypto-map)# match address 110
```

crypto ACL
Which specifies which traffic should be protected by Ipsec (interesting traffic)



Apply the crypto map on the outgoing interface

- Bind the VPN-MAP crypto map to the outgoing Serial 0/0/0 interface.

```
R1(config)# interface s0/0/0
```

```
R1(config-if)# crypto map VPN-MAP
```



Configure IPsec VPN settings on R3



1

Enable the Security Technology package

2

Identify interesting traffic on Router

3

Configure the IKE Phase 1 ISAKMP policy

4

Configure the IKE Phase 2 IPsec policy

5

Configure the crypto map

1

Enable the Security Technology package

- ▶ On R3, issue the **show version command** to view the Security Technology package license information.
- ▶ If the Security Technology package has not been enabled, use the following command to enable the package.
- ▶ R3(config)# **license boot module c1900 technology-package securityk9**
- ▶ Accept the end-user license agreement.(**type yes**)
- ▶ **Save the running-config**
- ▶ **reload** the router to enable the security license.
- ▶ **Verify** that the Security Technology package has been enabled by using the **show version command**

view the Security Technology package

► show version

```
License Info:

License UDI:

-----
Device#      PID                SN
-----
*0           CISCO1941/K9          FTX1524C38B-

Technology Package License Information for Module:'c1900'

-----
Technology    Technology-package    Technology-package
              Current      Type                Next reboot
-----
ipbase        ipbasek9             Permanent          ipbasek9
security      securityk9            Evaluation          securityk9
data          disable              None                None

Configuration register is 0x2102

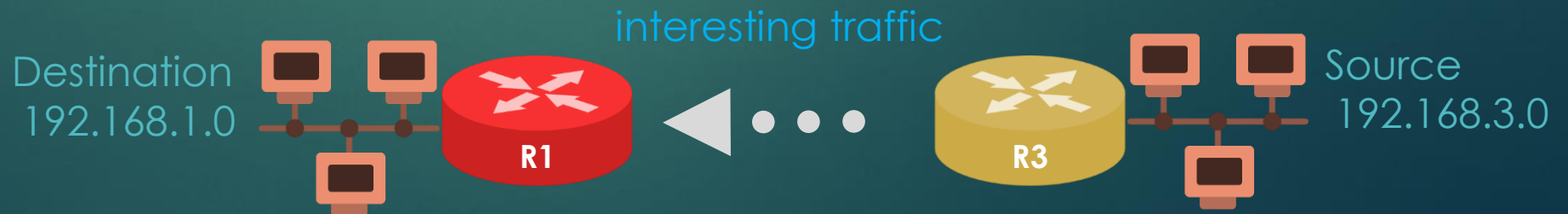
Router>
```



2

Identify interesting traffic on R1

- ▶ Configure **ACL 110** to identify the traffic from the LAN on R3 to the LAN on R1 **as interesting**.
- ▶ This interesting traffic will trigger the **IPsec VPN** to be implemented when there is traffic between the R3 to R1 LANs.
- ▶ All other traffic sourced from the LANs will not be encrypted. Because of the implicit deny all, there is no need to configure a deny ip any statement.
- ▶ R3(config)# **access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255**



3

Configure the IKE Phase 1 ISAKMP policy

- ▶ Configure the **crypto ISAKMP policy 10** properties on R3 along with the shared crypto key **cisco123**.
- ▶ Refer to the **ISAKMP Phase 1 table** for the specific parameters to configure. **Default values do not have to be configured**. Therefore, only the encryption method, key exchange method, and DH method must be configured.
- ▶ Note: The highest DH group currently supported by Packet Tracer is **group 5**.
In a production network, you would configure at least DH 14.

```
R3(config)# crypto isakmp policy 10
```

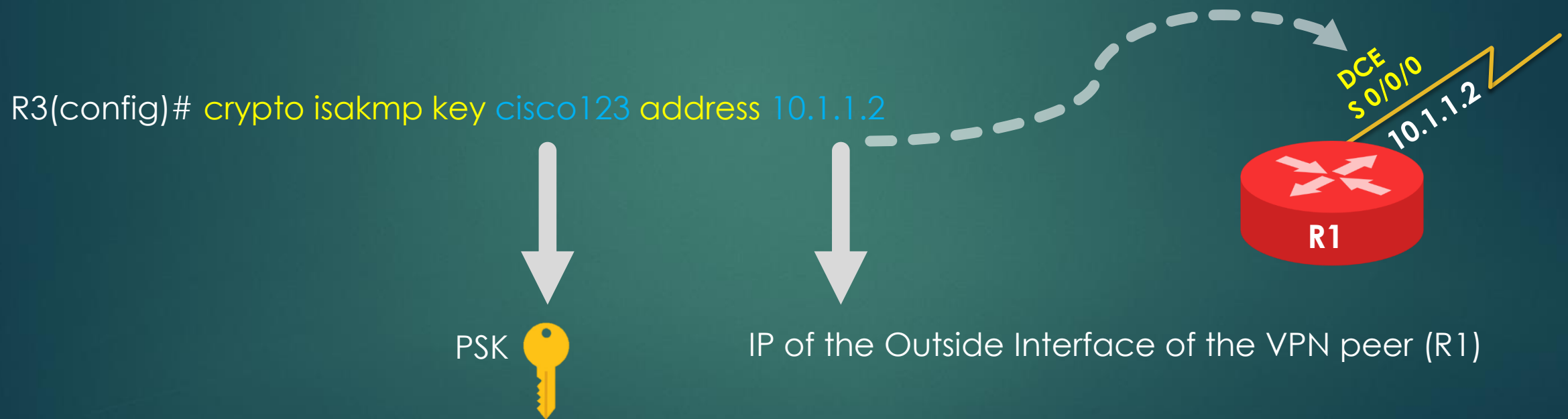
```
R3(config-isakmp)# encryption aes 256
```

```
R3(config-isakmp)# authentication pre-share
```

```
R3(config-isakmp)# group 5
```

Configure the pre-shared key (PSK)

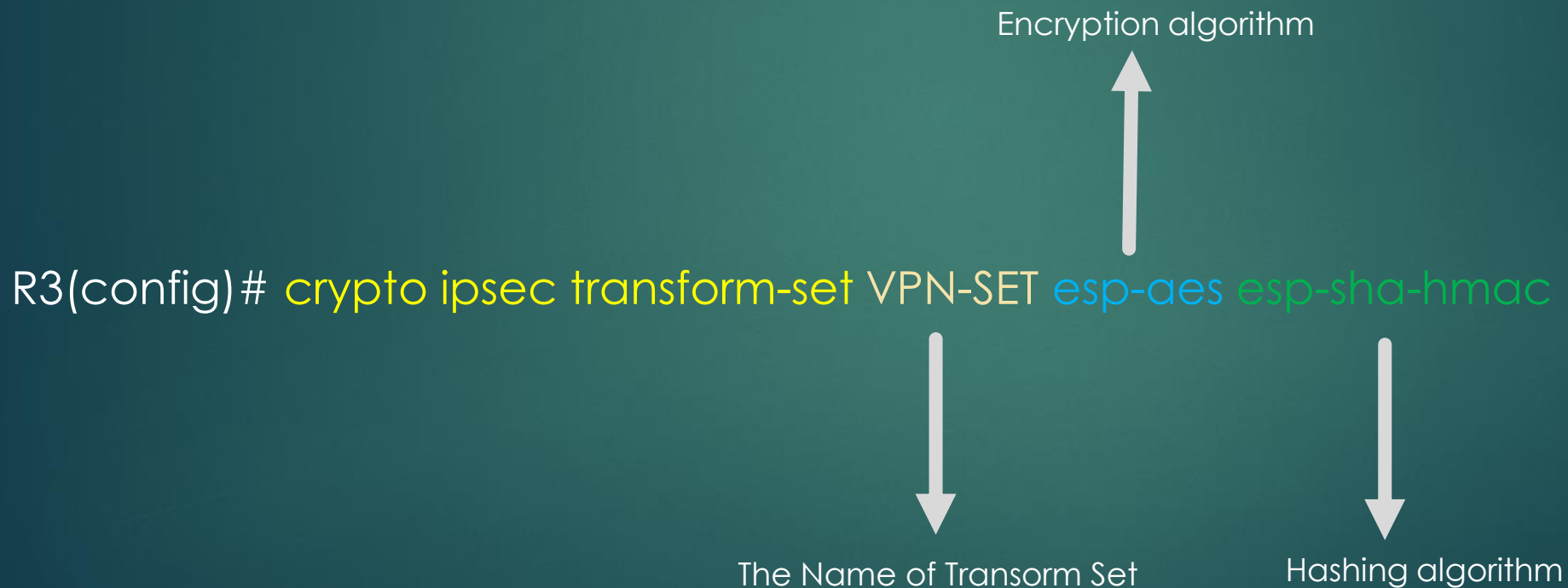
- ▶ The PSK allow the VPN peers to authentication each other



4

Configure the IKE Phase 2 IPsec policy

- The set of encryption and hashing algorithm that will be used to transform data sent through the IPsec Tunnel. This is called the transform set.



5

Configure the crypto map

- Create the **crypto map VPN-MAP** that binds all of the **Phase 2 parameters** together. Use sequence number 10 and identify it as an ipsec-isakmp map.

```
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
```

```
R3(config-crypto-map)# description VPN connection to R1
```

```
R3(config-crypto-map)# set peer 10.1.1.2
```

```
R3(config-crypto-map)# set transform-set VPN-SET
```

```
R3(config-crypto-map)# match address 110
```

crypto ACL
Which specifies which traffic
should be protected by Ipsec
(interesting traffic)

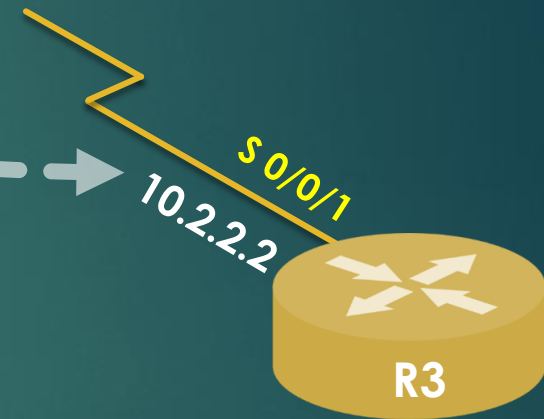


Apply the crypto map on the outgoing interface.

- Bind the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface.

```
R3(config)# interface s0/0/1
```

```
R3(config-if)# crypto map VPN-MAP
```



Part 2-C

Verify the IPsec VPN

Using show crypto ipsec sa command

- 1 Verify the tunnel prior to interesting traffic**
Issue the `show crypto ipsec sa` command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are **all set to 0**



```
R1# show crypto ipsec sa ddr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
  PERMIT, flags={origin is acl.}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0(0)

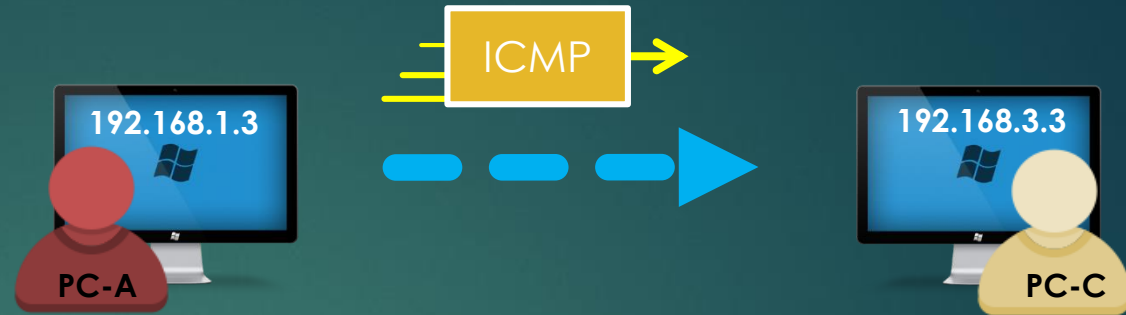
inbound esp sas:

inbound ah sas:
```

2

Create interesting traffic

Ping PC-C from PC-A



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.3.3
```

Pinging 192.168.3.3 with 32 bytes of data:

```
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
```

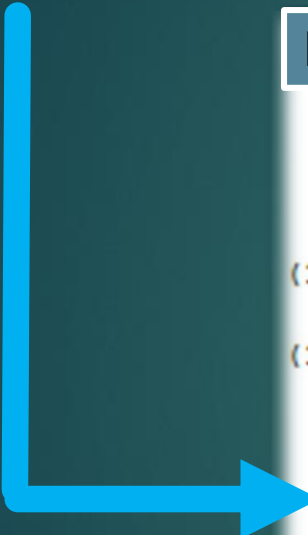
Ping statistics for 192.168.3.3:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms
```

3

Verify the tunnel after interesting traffic

On R1, re-issue the `show crypto ipsec sa` command. Notice that the number of packets is **more than 0**, which indicates that the IPsec VPN tunnel is working



```
R1# show crypto ipsec sa
```

```
Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
  PERMIT, flags={origin is acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

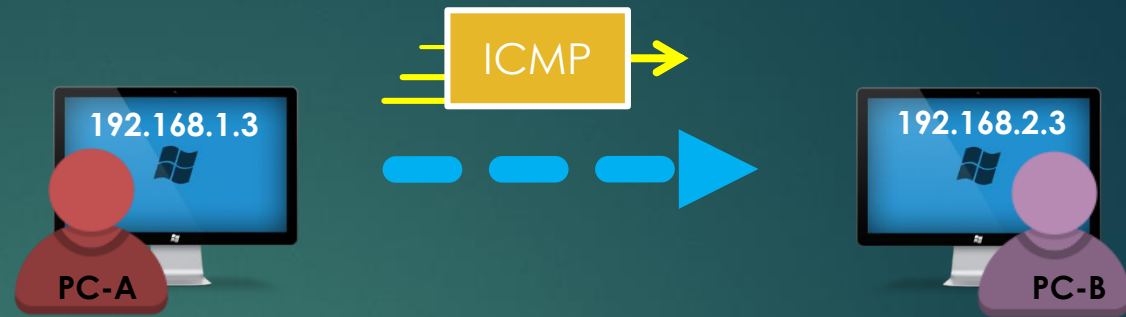
local crypto endpt.: 10.1.1.2, remote crypto endpt.: 10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0FCF73A6(265253798)

inbound esp sas:
  spi: 0x63113A4F(1662073423)
--More--
```

4

Create uninteresting traffic

Ping PC-B from PC-A



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.2.3
```

Pinging 192.168.2.3 with 32 bytes of data:

```
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=4ms TTL=126
Reply from 192.168.2.3: bytes=32 time=2ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
```

Ping statistics for 192.168.2.3:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

5

Verify the tunnel after uninteresting traffic

On R1, re-issue the `show crypto ipsec sa` command. Notice that the number of packets has **not changed**, which verifies that uninteresting traffic is not encrypted.

R1# show crypto ipsec sa

```
Crypto map tag: VPN-MAP, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
PERMIT, flags={origin is acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0FCF73A6(265253798)

inbound esp sas:
spi: 0x63113A4F(1662073423)
--More--
```



The End

***I hope you will have to
understand and enjoy***

With all respect and appreciation to you

*By Eng. Ala'aldin Sweilem
Network Trainer
Alaswelm2013@gmail.com*