Computer Networking: Beyond Routing & Switching Series

- **Next Session*: Intro to Data Centers*** Tuesday, November 10, 2015 8:00 am, PST, REGISTER HERE

Join for an introduction to the concept of a datacenter from a holistic perspective (hardware, software, processes) with a focus on virtualization and cloud. We will also discuss the challenges that IT departments face and look at the trends in datacenter technologies!

- 3rd Session: ***Going Wireless – Wireless Communications and Technologies – Dec. 8th, 2015, 9:00 P.M. PST***

Mapping Your Path to Success

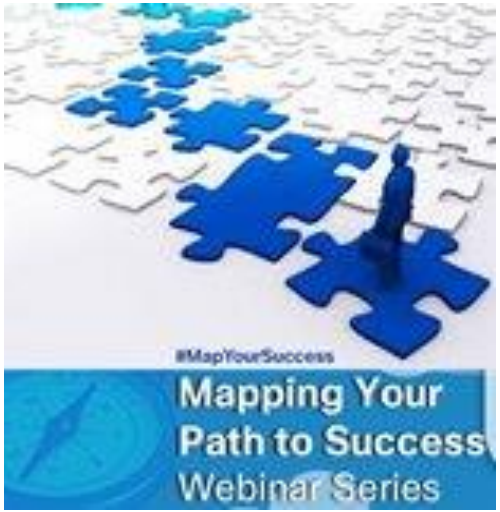
Upcoming Sessions:

- The Art of Persuasion & Influencing People

  November 4th 2015 – 9:00 PM PST, REGISTER HERE

- The Power of Public Speaking

  November 18th 2015 – 9:00 PM PST, REGISTER HERE



Future Sessions cover Teamwork, Becoming Inspired!, and Communicating Effectively with Body Language

Internet of Everything Webinar Series

TOPIC
IoE Cloud & Mobility

DATE
October 21st, 8:00 AM PST

REGISTER HERE

TOPIC
IoE & Smart Cities

DATE
November 12th , 8:00 AM & 8:00 P.M. PST

8:00 A.M. PST: REGISTER HERE

8:00 P.M. PST: REGISTER HERE

Introduction to Cybersecurity and VPN Tunnels

Professor Kerry-Lynn Thomson

Nelson Mandela Metropolitan University (NMMU)

Port Elizabeth, South Africa

Agenda

- Introduction to Cybersecurity
- Generic Route Encapsulation (GRE) Tunnels
- Internet Protocol Security (IPSec) Tunnels

What is Cybersecurity?

"Adversaries are committed to continually refining or developing new techniques that can evade detection and hide malicious activity.

Meanwhile, the defenders—namely, security teams—must constantly improve their approach to protecting the organization and users from these increasingly sophisticated campaigns.

Caught in the middle are the users. But now, it appears they not only are the targets, but also the complicit enablers of attacks."

Cisco Annual Security Report, 2015

The Scale of Malicious Cyber Activity

317 MILLION NEW PIECES OF MALWARE

NEARLY 2.4 TIMES AS MANY BABIES BORN EACH YEAR

Almost **1 MILLION**

PIECES OF MALWARE PER DAY

12 PIECES OF SOFTWARE PER SECOND

2015 Internet Security Threat Report (Symantec)

The Scale of Malicious Cyber Activity

Ransomware attacks increased by 113%

Crypto-Ransom attacks rose 4000%

70% of social media attacks rely on initial victim to spread threat

2015 Internet Security Threat Report (Symantec)

The Global Price Tag of Consumer Cybercrime

Global Price Tag of Cybercrime

Total = $375 billion - $1 trillion

Global black market in marijuana, cocaine and heroin combined = $450 billion

All global drug trafficking = $600 billion

Cybersecurity Professionals

Demand for cybersecurity professionals has grown more than 3.5x faster than the demand for other IT jobs over the past 5 years

Demand has grown more than 12x faster than the demand for all other non-IT jobs

Burning Glass Technologies

Introduction to Cybersecurity

Cybersecurity Course Overview

- Introduces the importance of cybersecurity and current trends
- Not intended to teach students to implement security products and processes - but rather to raise awareness of the global need for cybersecurity and the advancements in the industry
- This course is intended for individuals who have, at least, a basic understanding of networking concepts

- 8 modules with presentations and panel discussions that feature industry experts
- Activities, videos, and additional resources for students to explore

- Final exam – Certificate of Completion
- Estimated time to complete: 13-15 hours

Cybersecurity Course Overview

Module	Goals
1. The Cybersecurity Industry	- Explain the importance of cybersecurity in the global economy - Explain why cybersecurity is a growing profession

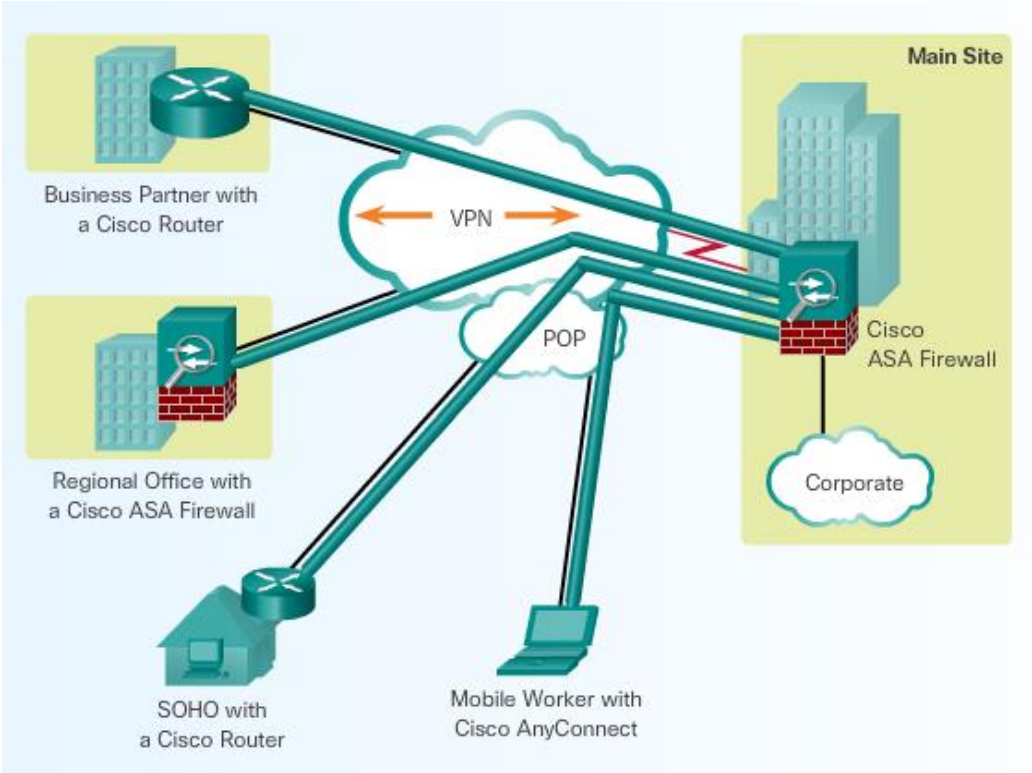
Cybersecurity Course Overview

Module	Goals
5. Defending Against Global Threats	- Explain the characteristics of cyber warfare - Explain how Cisco Security Intelligence Operations (SIO) tracks and responds to a global threat

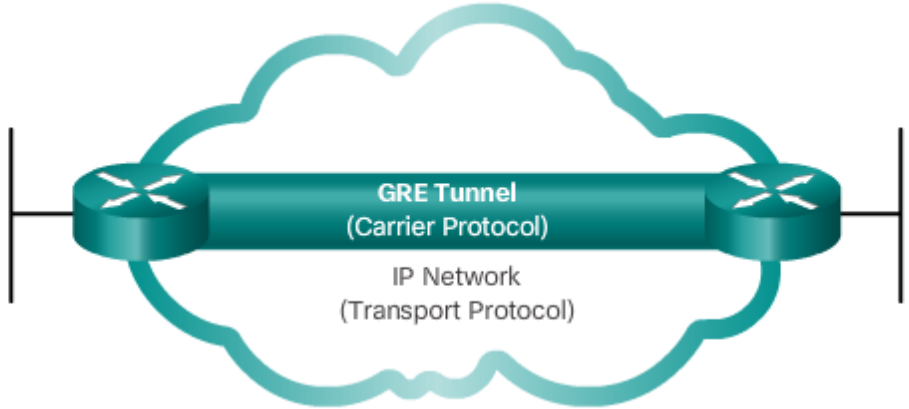
CCNA Security – VPN Tunnels

Site-to-Site and Remote-Access VPNs

What is a Virtual Private Network (VPN)?



Generic Routing Encapsulation (GRE) Tunnels

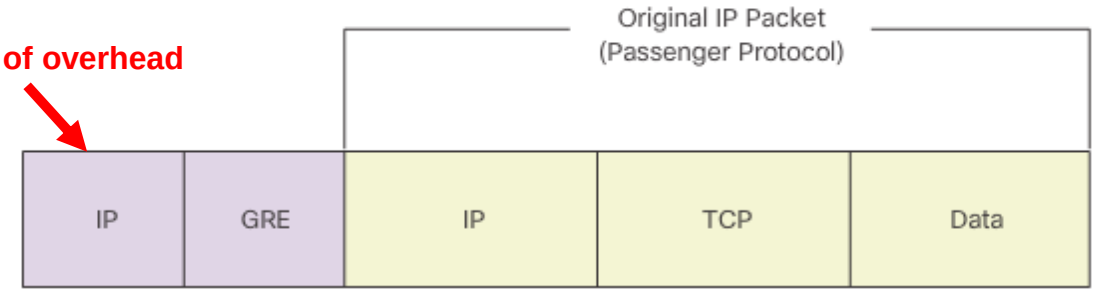


User Traffic: IP or other Layer 3 protocol

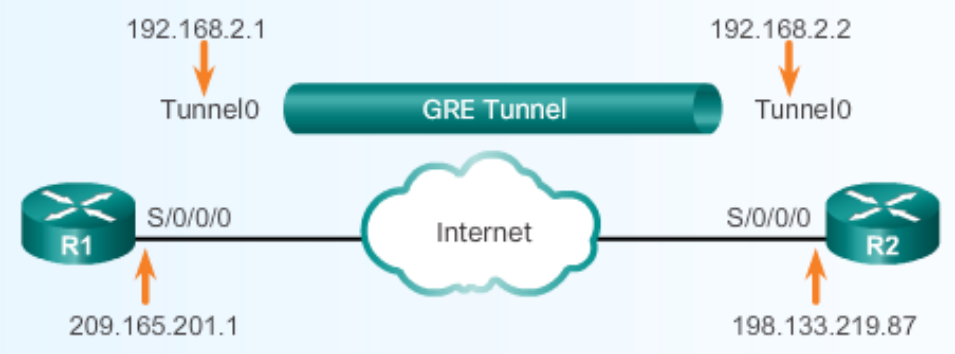
Type of traffic: Unicast or Multicast

Confidentiality: NO

24 bytes of overhead



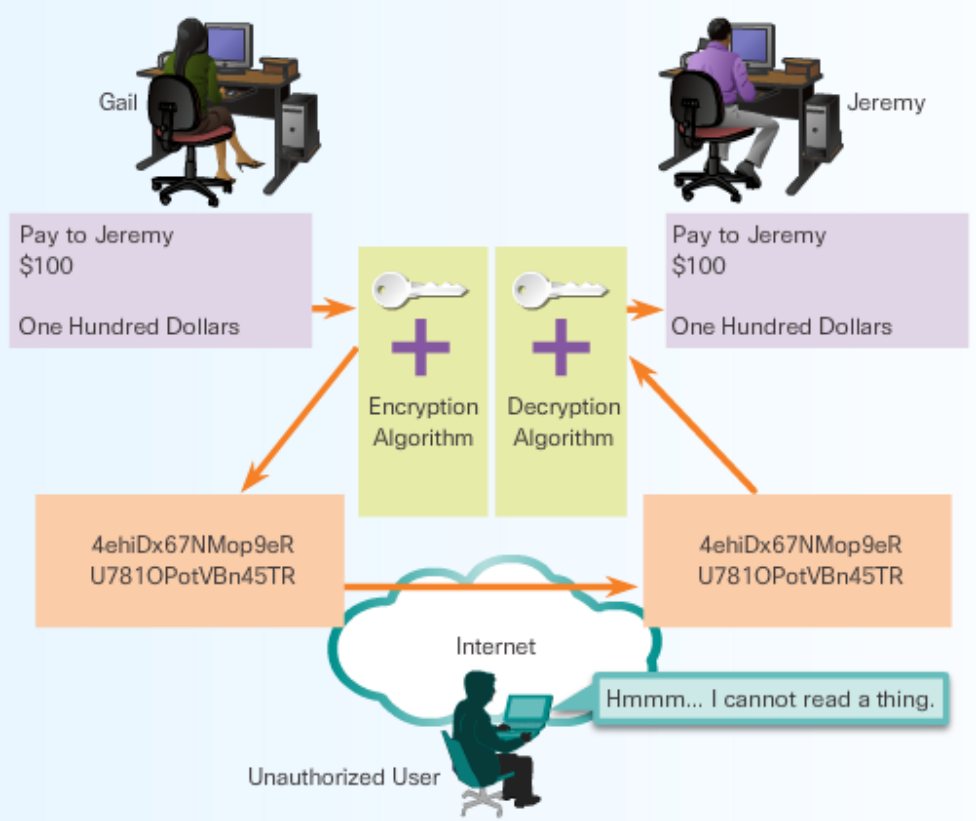
GRE Configuration




```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

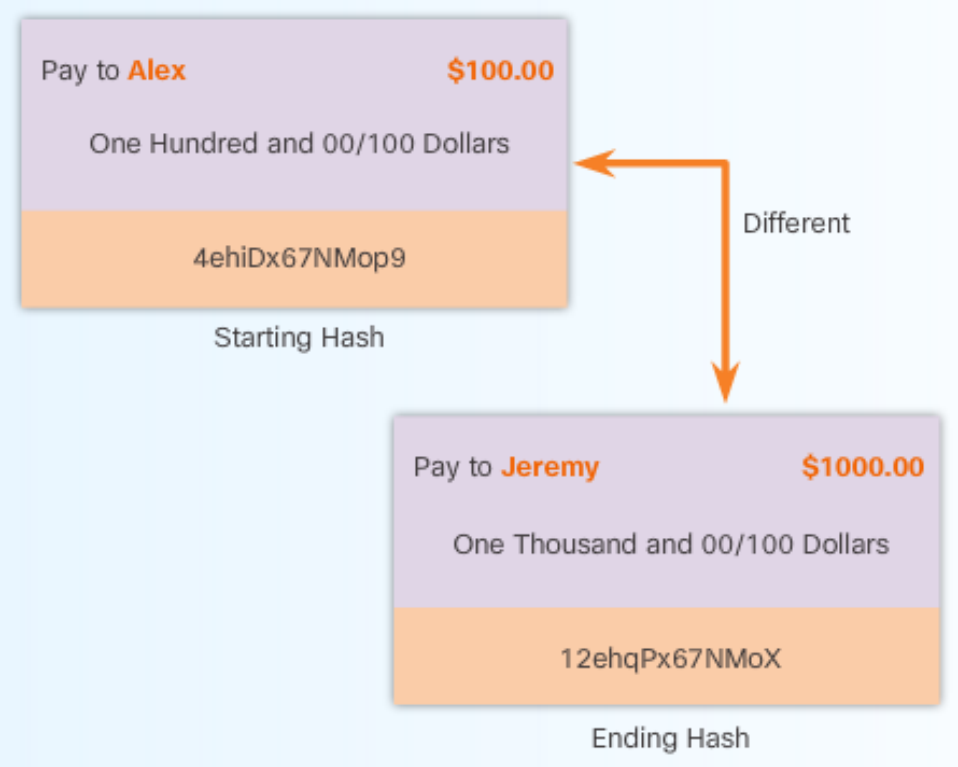
Confidentiality with Encryption



Symmetric Keys

DES, 3DES, AES

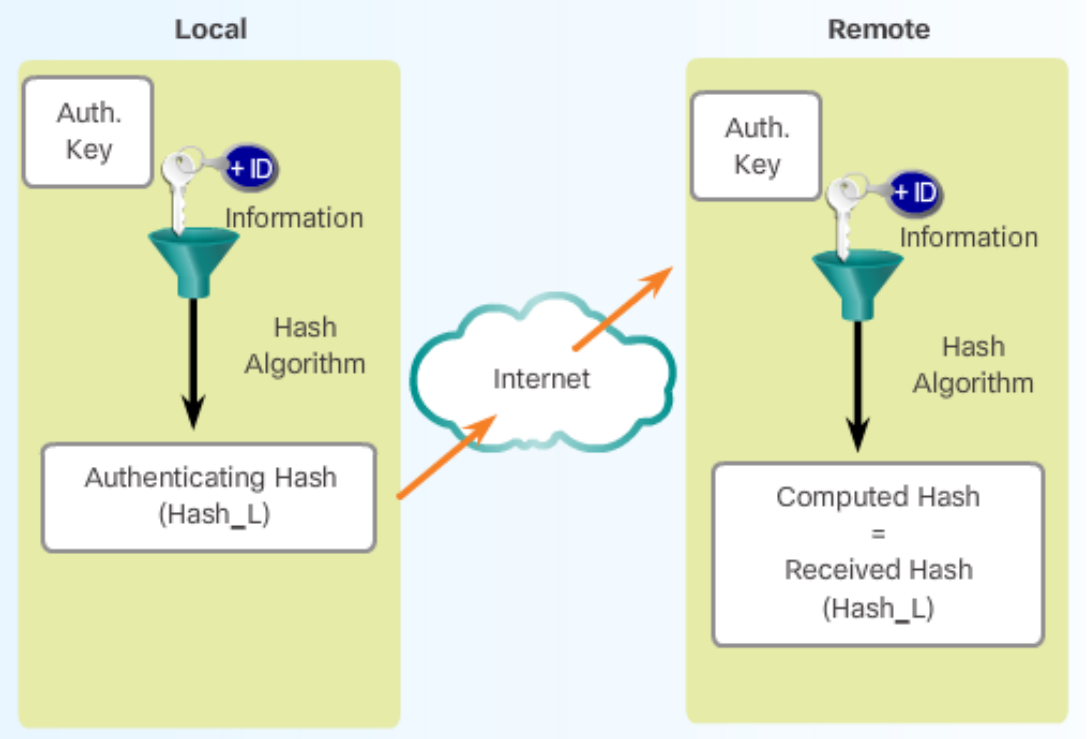
Integrity through Hashing



MD5 – 128 bits

SHA – 160 bits

Authentication through Pre-Shared Keys (Symmetric Keys)



Manually entered

Authentication key is hashed and sent to peer

Introducing IPSec

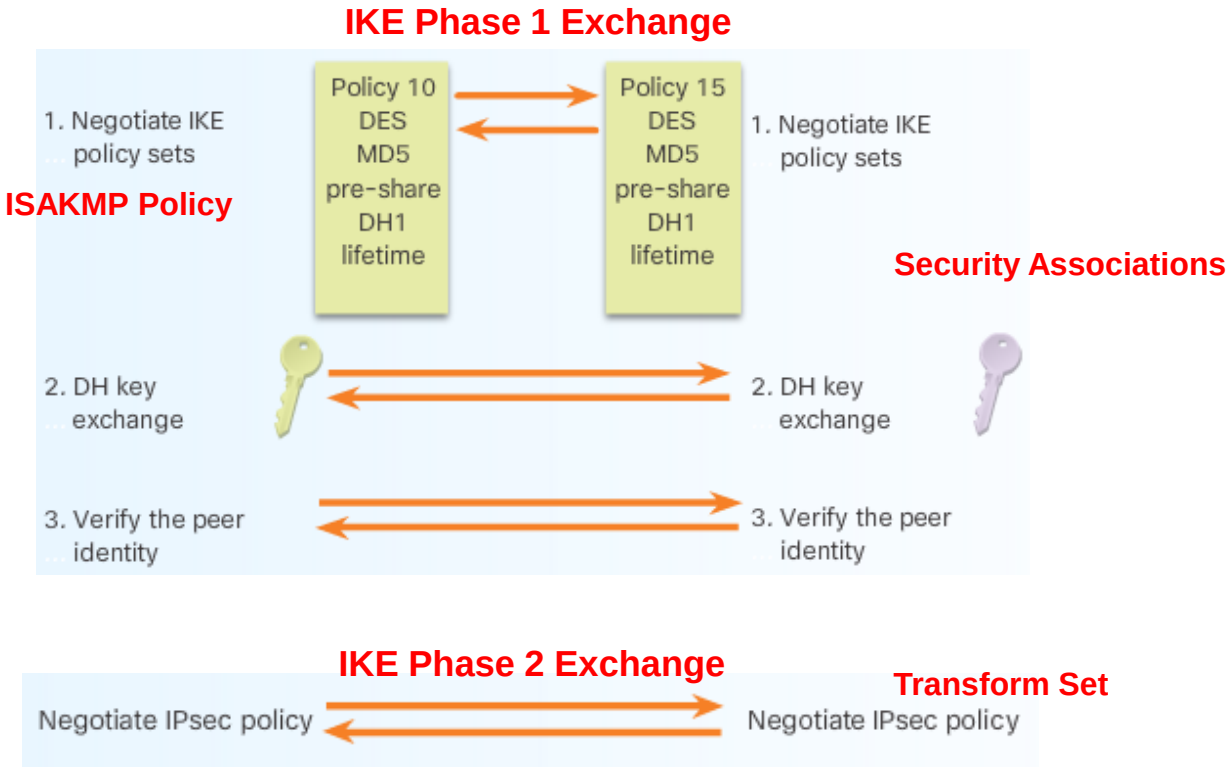
User Traffic: IP

Type of traffic: Unicast

Confidentiality: YES (ESP)

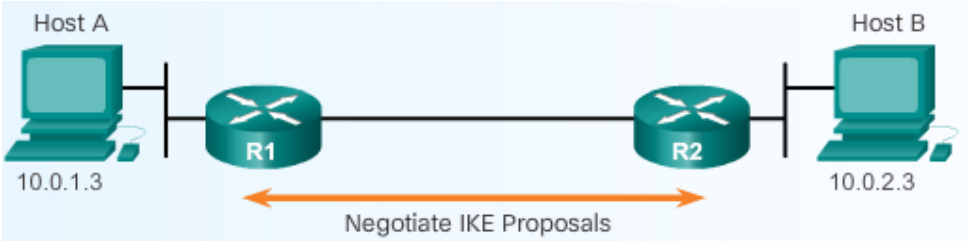
If need to run routing protocols or different user traffic – but still need security – can run IPSec with GRE tunnel

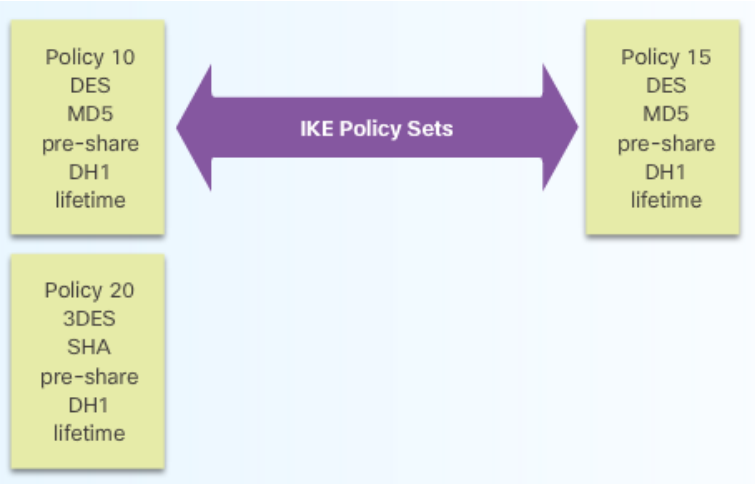
IKE (Internet Key Exchange) Phase 1 and Phase 2



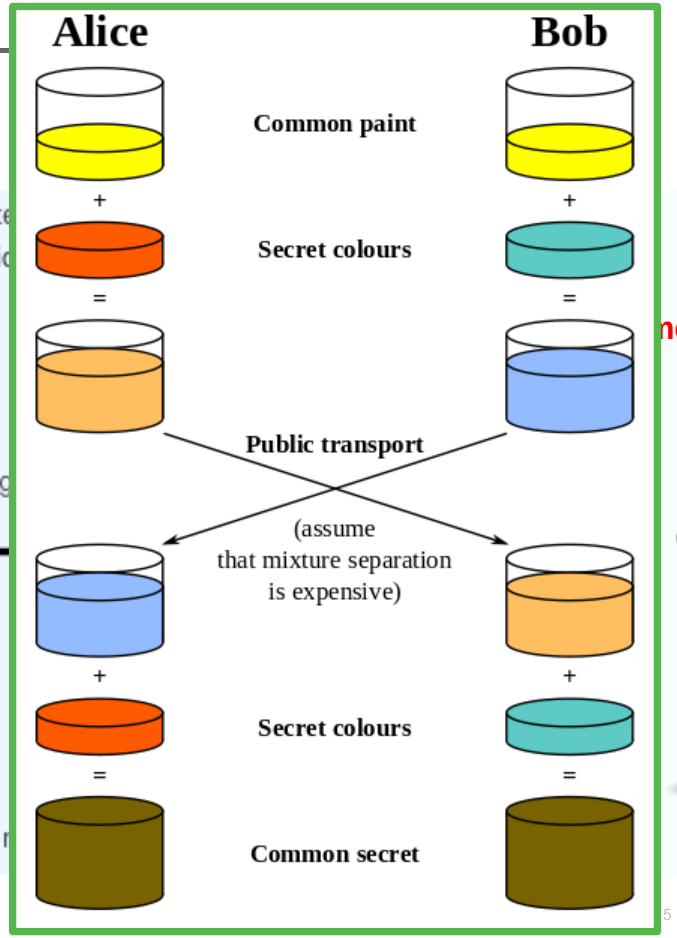
1st Exchange – ISAKMP Policy Negotiation

Internet Security Association and Key Management Protocol

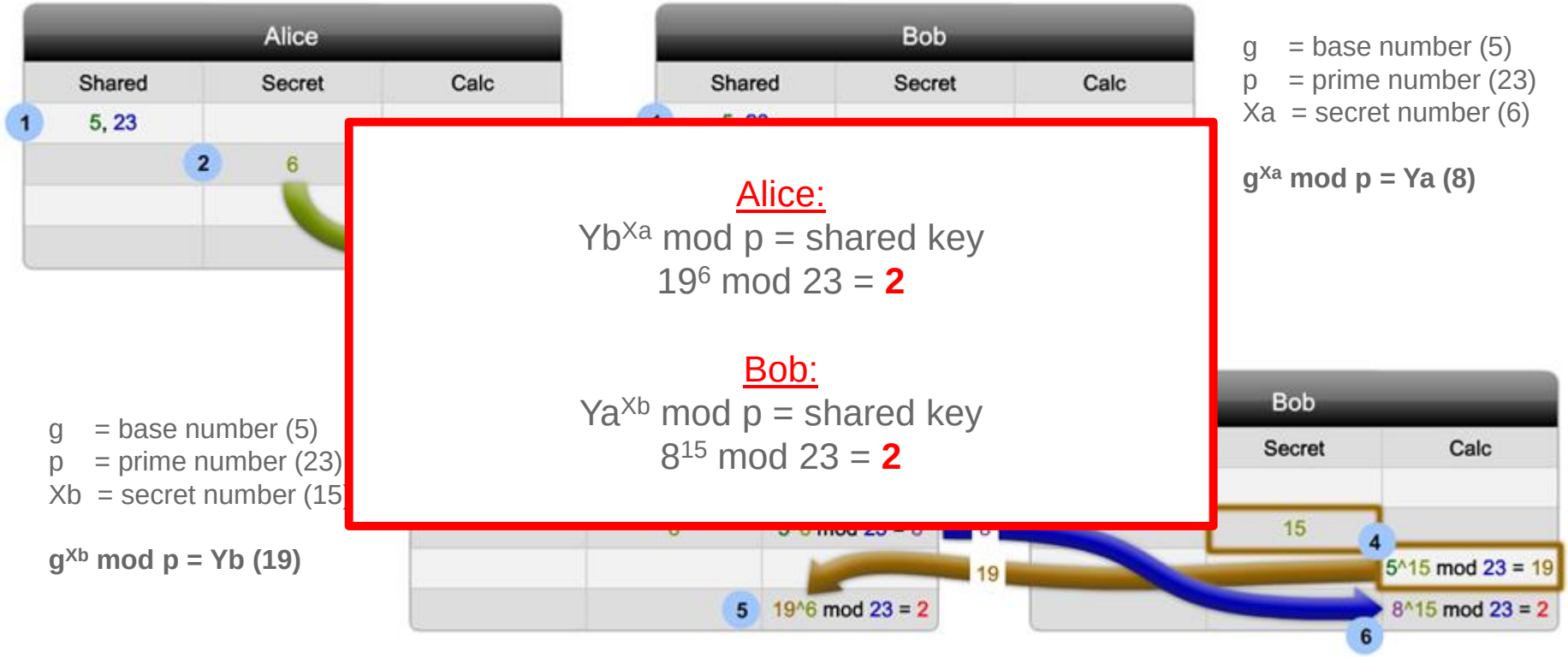




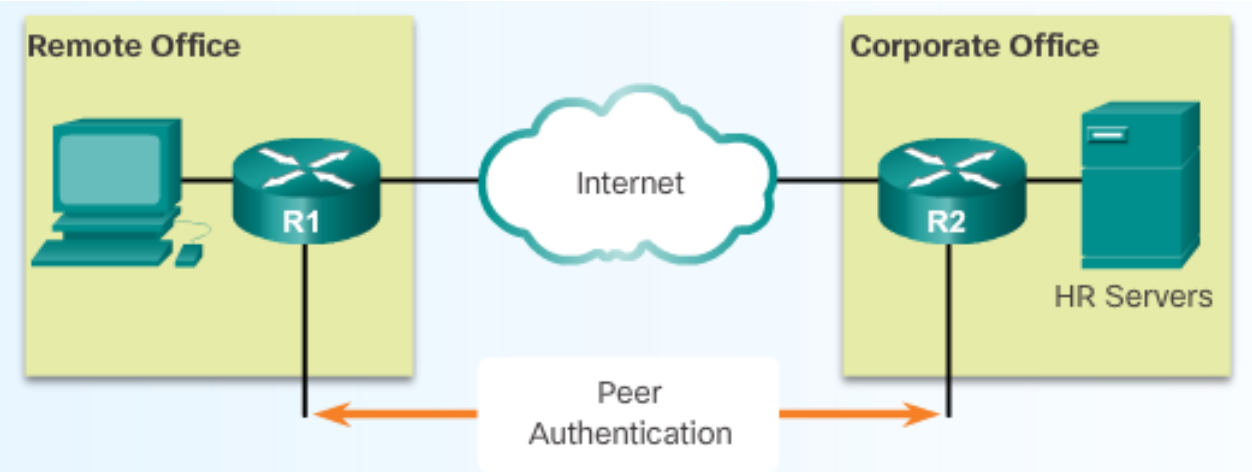
2nd Exchange -



Diffie-Hellman Key Exchange



3rd Exchange – Peer Authentication



PSK
RSA Signatures

This ends IKE Phase 1!!

`show crypto isakmp sa` = QM_IDLE

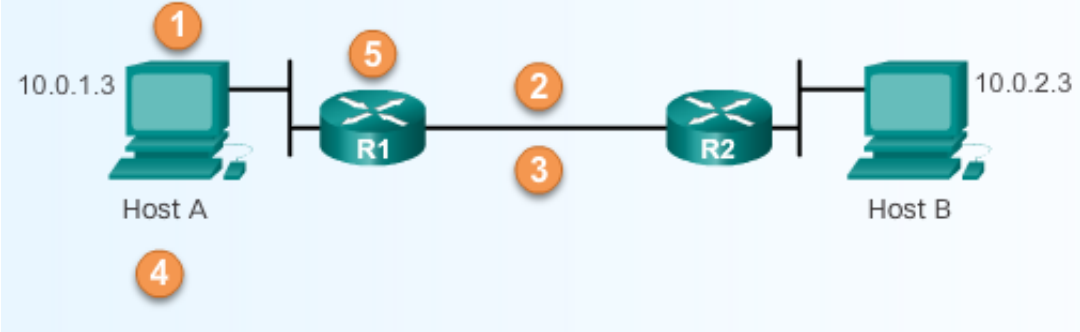
IKE Phase 2

Quick mode – will not initiate if Phase 1 is not complete!!

as defined in Transform Set

`show crypto ipsec sa` = # of packets encrypted and decrypted

IPSec VPN Negotiation – Building the Tunnel



1. **Host A sends *'interesting traffic'* to Host B**
2. **R1 and R2 negotiate an IKE Phase 1 session**
3. **R1 and R2 negotiate an IKE Phase 2 session**
4. **Information is exchanged via IPSec tunnel**
5. **IPSec tunnel is terminated**

Tasks to Configure IPSec

Task 1: **Ensure that ACLs configured on interfaces are compatible with the IPSec configuration**

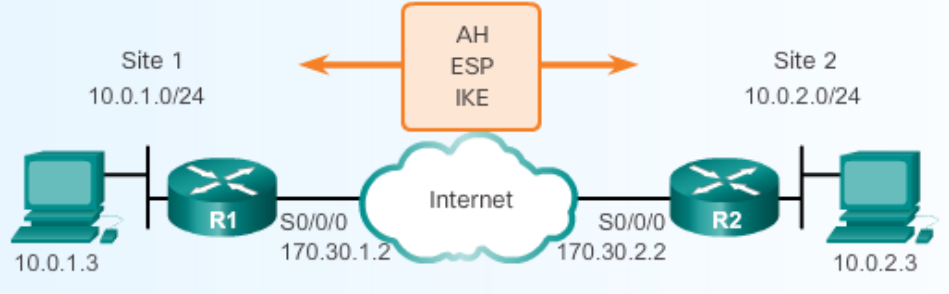
Task 2: **Create an ISAKMP (IKE) policy**

Task 3: **Configure an IPSec transform set**

Task 4: **Create a crypto ACL**

Task 5: **Create and apply the crypto map**

Task 1 – Configure Compatible ACLs

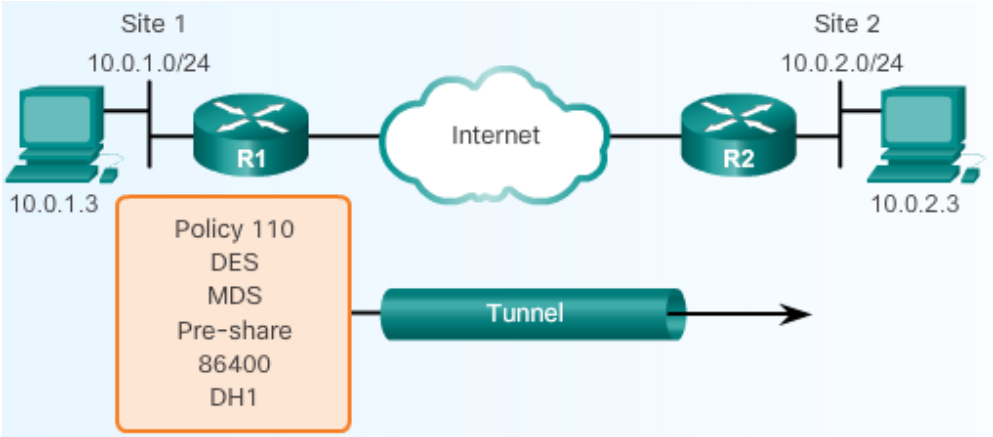



```
R1(config)# access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq
 isakmp
R1(config)# interface Serial0/0/0
R1(config-if)# ip address 172.30.1.2 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# ip access-group 102 in
R1(config-if)# exit
R1(config)# exit
R1#
R1# show access-lists
    access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
```

Phase 2

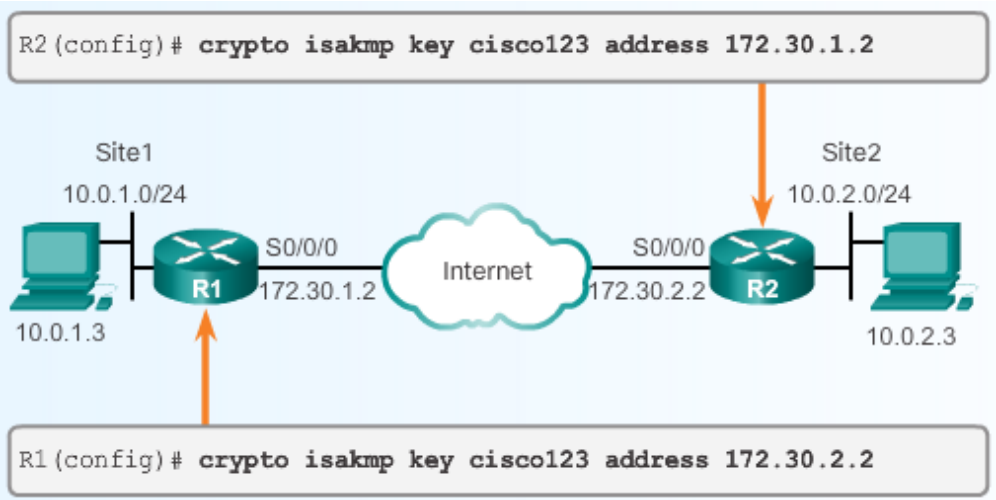
Phase 1

Task 2 – Configure IKE




```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption des
R1(config-isakmp)# group 1
R1(config-isakmp)# hash md5
R1(config-isakmp)# lifetime 86400
```

Pre-Shared Keys



Task 3 – Configure the Transform Sets

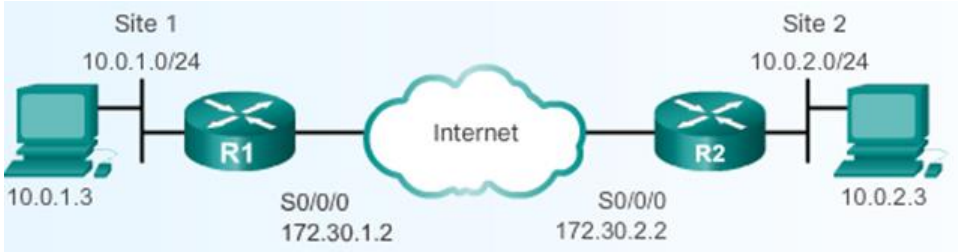
IKE Phase 2 Quick Mode

```
R1(config)# crypto ipsec transform-set MYSET esp-aes 128
```

```
R2(config)# crypto ipsec transform-set OTHERSET esp-aes 128
```

Task 4 – Crypto ACL

Defining Interesting Traffic

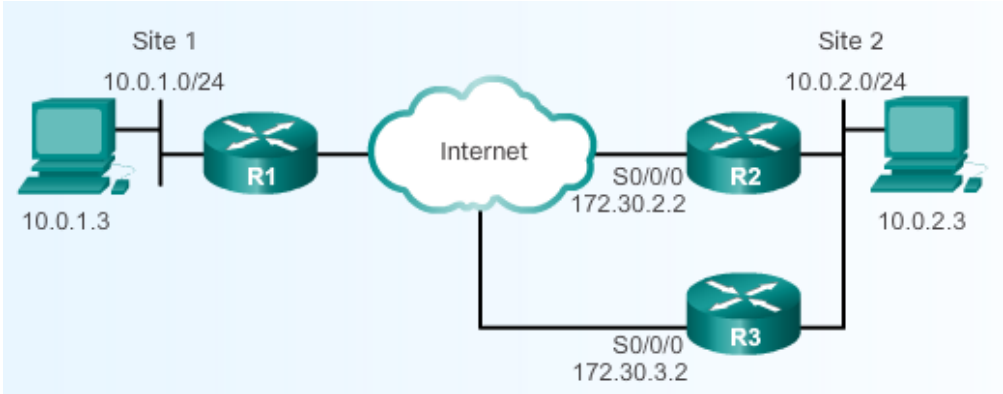



```
R1(config)# access-list 110 permit tcp 10.0.1.0 0.0.0.255
  10.0.2.0 0.0.0.255
```

```
R2(config)# access-list 101 permit tcp 10.0.2.0 0.0.0.255
  10.0.1.0 0.0.0.255
```

!!Crypto ACLs must be mirrors!!

Task 5 – Define and Apply Crypto Map




```
R1(config)# crypto map MYMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2 default
R1(config-crypto-map)# set peer 172.30.3.2
R1(config-crypto-map)# set pfs group1
R1(config-crypto-map)# set transform-set MYSET
R1(config-crypto-map)# set security-association lifetime seconds 86400
```

```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map MYMAP
```

Thank you for your attention!

Prof Kerry-Lynn Thomson

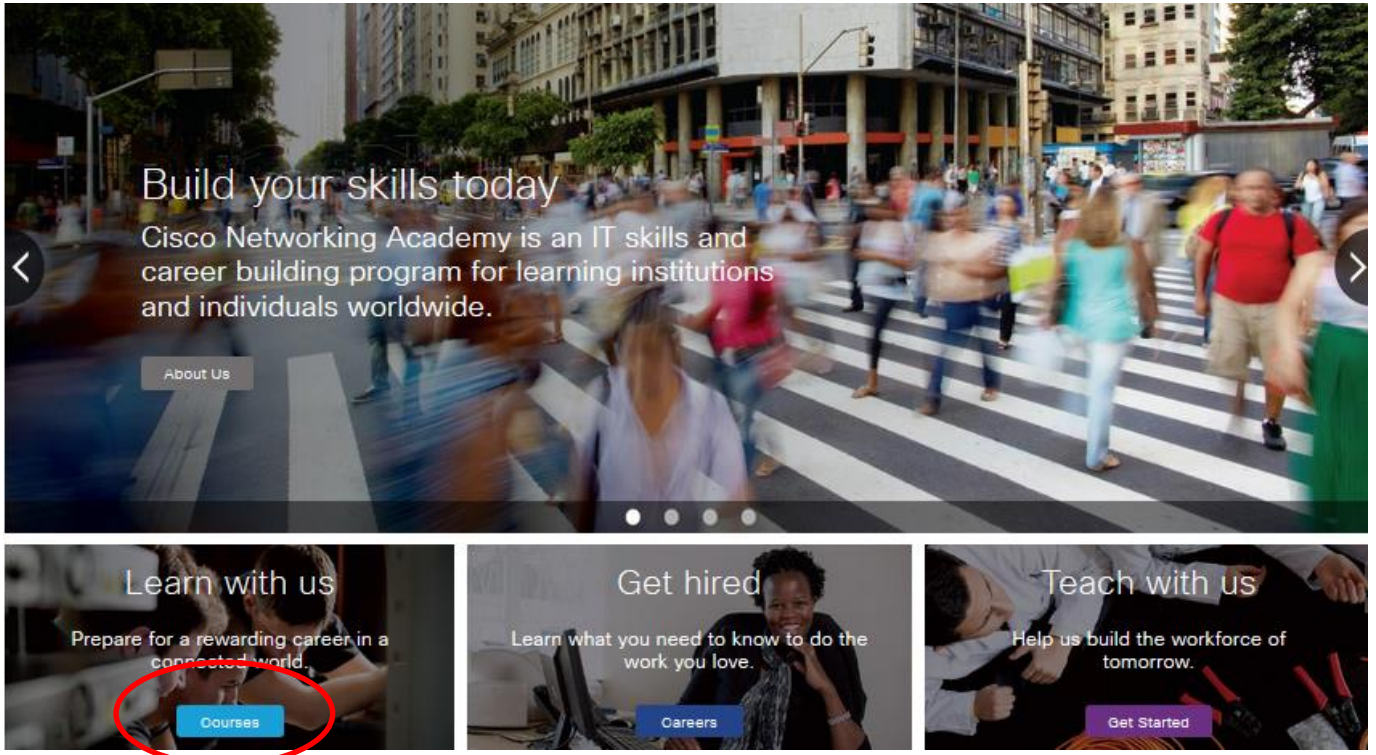
kerry-lynn.thomson@nmmu.ac.za

Start Your Cybersecurity Training Today!

- Become a Cyberhero as shown in video!
- Sign up for Introduction to Cybersecurity *(from video)*
- Recruit others to join your cybersecurity league!

Join Cisco Networking Academy

- Go to netacad.com
- Click *Learn with Us*



TOMORROW starts here.