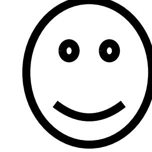
Branch Connections

- **GRE**
  - Implement a GRE tunnel.
- **VPNs**
  - Explain how VPNs secure site-to-site and remote access connectivity.
- **IPsec**
- Access Connections
  - Select broadband remote access technologies to support business requirements.
- PPPoE
  - Configure a Cisco router with PPPoE.
  - homed remote access network.
- eBGP
  - Implement eBGP in a single

VPNs

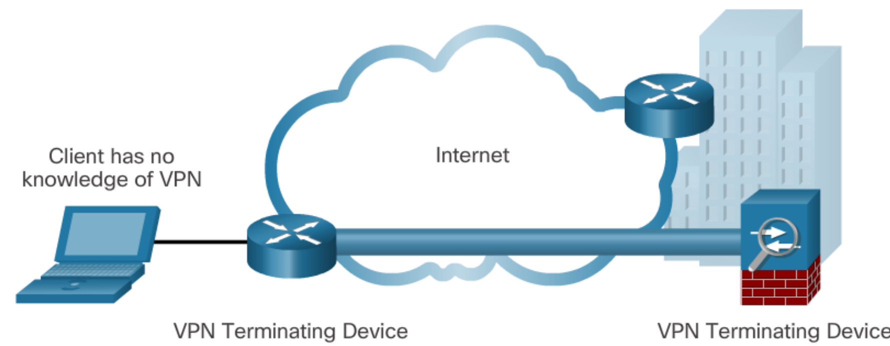
Fundamentals of VPNs

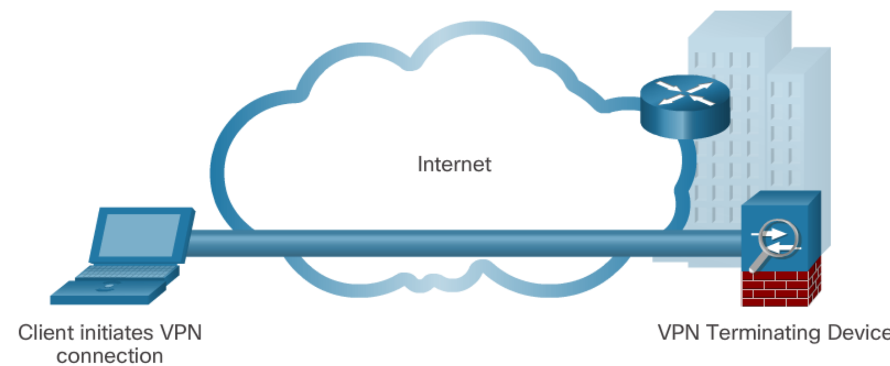


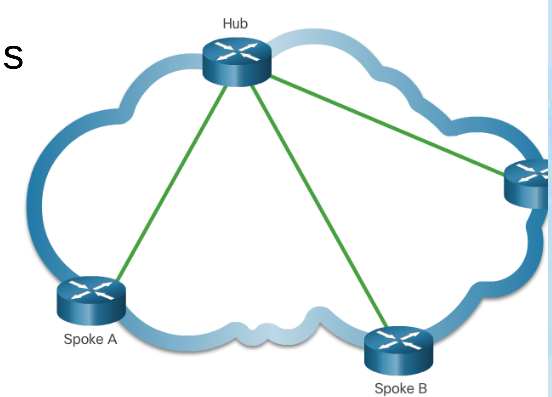
- Introducing VPNs
  - VPNs used to **create an end-to-end private network connection over the Internet**.
  - A secure implementation of **VPN with encryption** are **IPsec** VPNs.
  - **VPN gateways** could be a **router**, a **firewall**, or a Cisco Adaptive Security Appliance (**ASA**).
- Benefits of VPNs (compared to leased lines)
  - **Cost savings** – regular Internet transport
  - **Scalability** - easy to add new users
  - **Compatibility** - all broadband technologies for mobile workers and telecommuters
  - **Security** – encryption, integrity and authentication

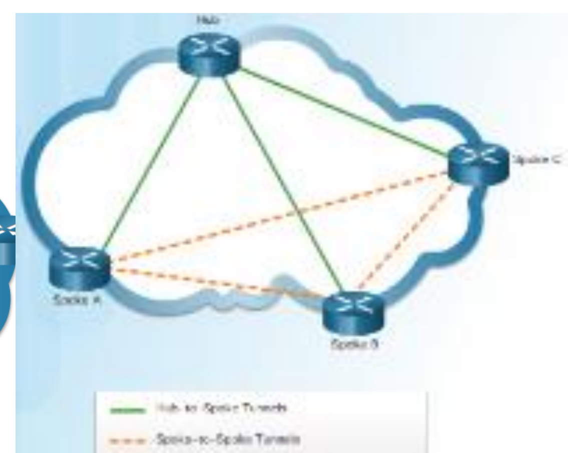
Types of VPNs

- Site-to-Site
  - **Site-to-site VPNs connect entire networks to each other**, for example, they can connect a branch office network to a company headquarters network.
- Remote Access
  - Remote-access VPNs are used **to connect individual hosts** that must access their company network securely over the Internet.
- DMVPN
  - **Dynamic Multipoint VPN (DMVPN)** is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner.
    Hub and Spoke topology.





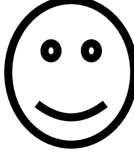


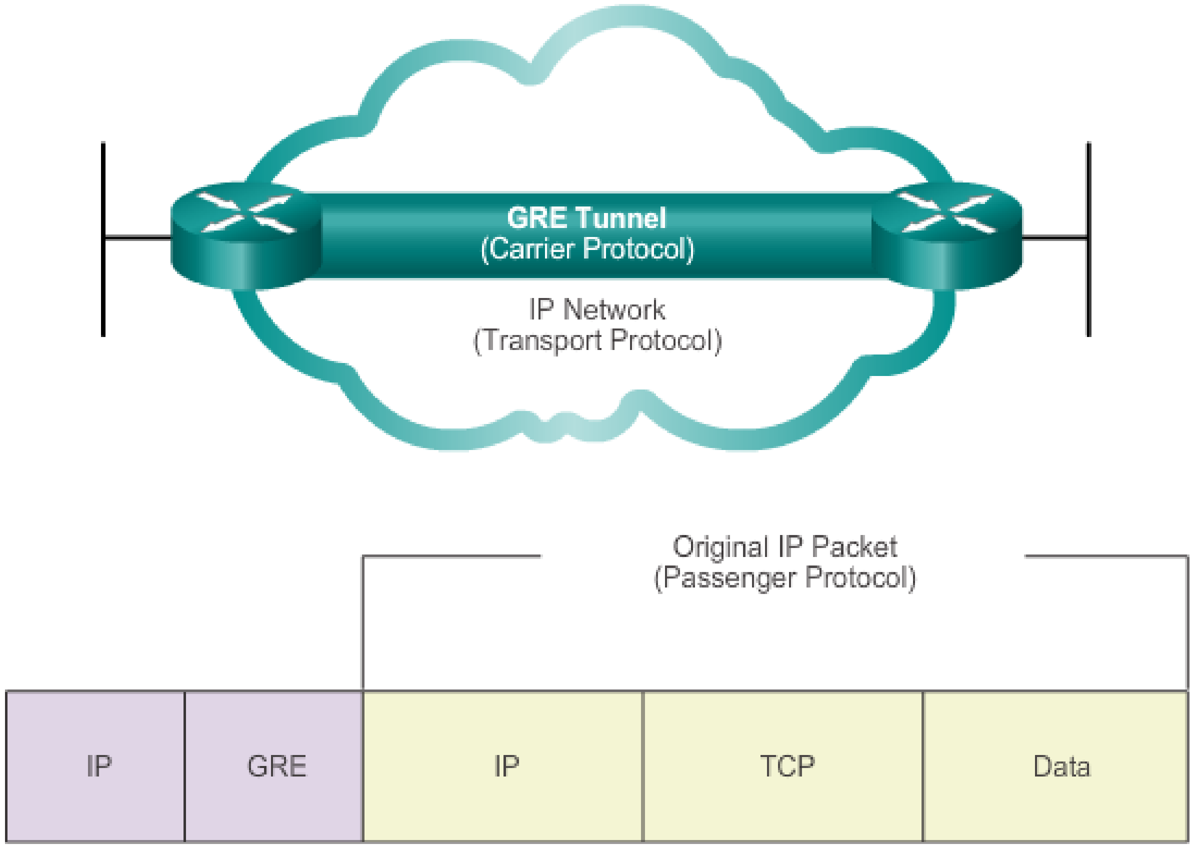


GRE – Generic Routing Encapsulation

GRE is a non-secure, site-to-site VPN tunneling protocol.

Generic Routing Encapsulation - GRE



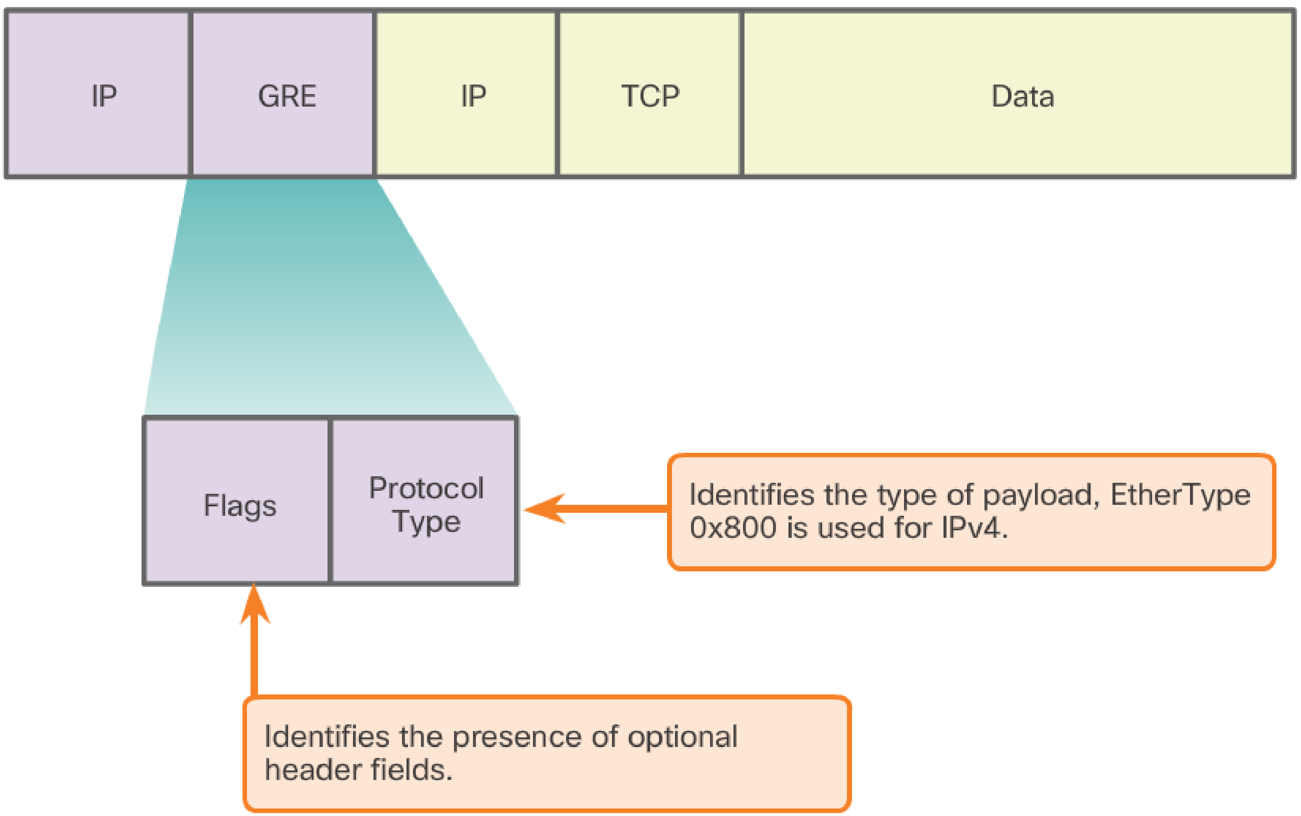


- Basic, **non-secure, site-to-site VPN tunneling protocol** developed by Cisco.
- **Encapsulates a wide variety of protocol packet types inside IP tunnels.**
- **Creates a virtual point-to-point link** to routers at remote points, **over an IP internetwork**.
- Used to deliver **IP multicast traffic** or **IPv6 traffic over an IPv4 unicast-only connection.**

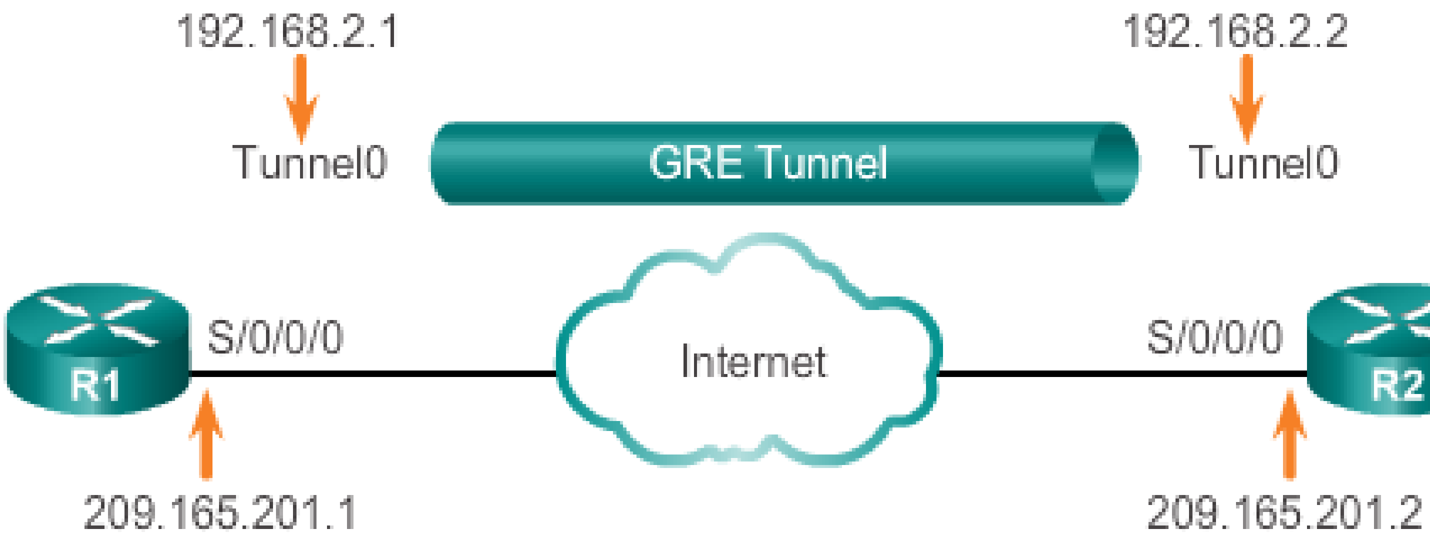
GRE

Generic Routing Encapsulation (GRE) is designed to manage the **transportation of multiprotocol and IP multicast traffic** between two or more sites, that may only have IP connectivity.

The **GRE header and** the **tunneling IP header create 24 bytes of additional overhead** for tunneled packets.



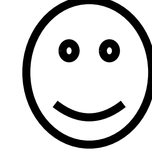
GRE Tunnel Configuration



R1 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 209.165.201.2
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Configuring GRE Tunnels
GRE Tunnel Configuration



R2 configuration:

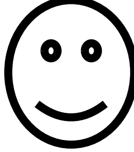
Achtung: besser Prefixlänge /30 verwenden.

```
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 209.165.201.2
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
```

Command	Description
`tunnel mode gre ip`	Specifies that the mode of the tunnel interface is GRE over IP.
`tunnel source ip_address`	Specifies the tunnel source address.
`tunnel destination ip_address`	Specifies the tunnel destination address.
`ip address ip_address mask`	Specifies the IP address of the tunnel interface.

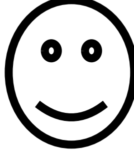
GRE

Implement GRE



- There are **five steps** to configuring a GRE tunnel:
  - **Step 1.** Create a tunnel interface using the **interface tunnel number** command.
  - **Step 2.** Configure an **IP address for the tunnel interface**.
    This is normally a private IP address.
  - **Step 3.** Specify the tunnel source IP address (an Internet address).
  - **Step 4.** Specify the tunnel destination IP address (an Internet address).
  - **Step 5.** (Optional) Specify GRE tunnel mode as the tunnel interface mode.

GRE Tunnel Verification



```
R1# show ip interface brief | include Tunnel

Tunnel0                    192.168.2.1     YES manual up         up
```

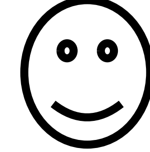
Verify Tunnel Interface is Up

```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP
<output omitted>
```

Verify OSPF Adjacency

```
R1# show ip ospf neighbor

Neighbor ID     Pri  State           Dead Time   Address         Interface
209.165.201.2   0    FULL/  -        00:00:37    192.168.2.2     Tunnel0
```

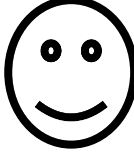
Implement GRE



- Verify GRE
  - To determine whether the tunnel interface is up or down, use the **show ip interface brief** command.
  - To verify the state of a GRE tunnel, use the **show interface tunnel** command.
  - Verify that an OSPF adjacency has been established over the tunnel interface using the **show ip ospf neighbor** command.

- Troubleshoot GRE
  - Use the **show ip interface brief** command on both routers to verify that the tunnel interface is up and configured with the correct IP addresses for the physical interface and the tunnel interface.
  - Use the **show ip ospf neighbor** command to verify neighbor adjacency.
  - Use **show ip route** to verify that networks are being passed between the two routers

IPsec VPNs



IPsec services allow for **CIA** = **C**onfidentiality, **I**ntegrity, and **A**uthentication.

CIA:
Confidentiality (Encryption) –
encrypt the data before transmitting across the network

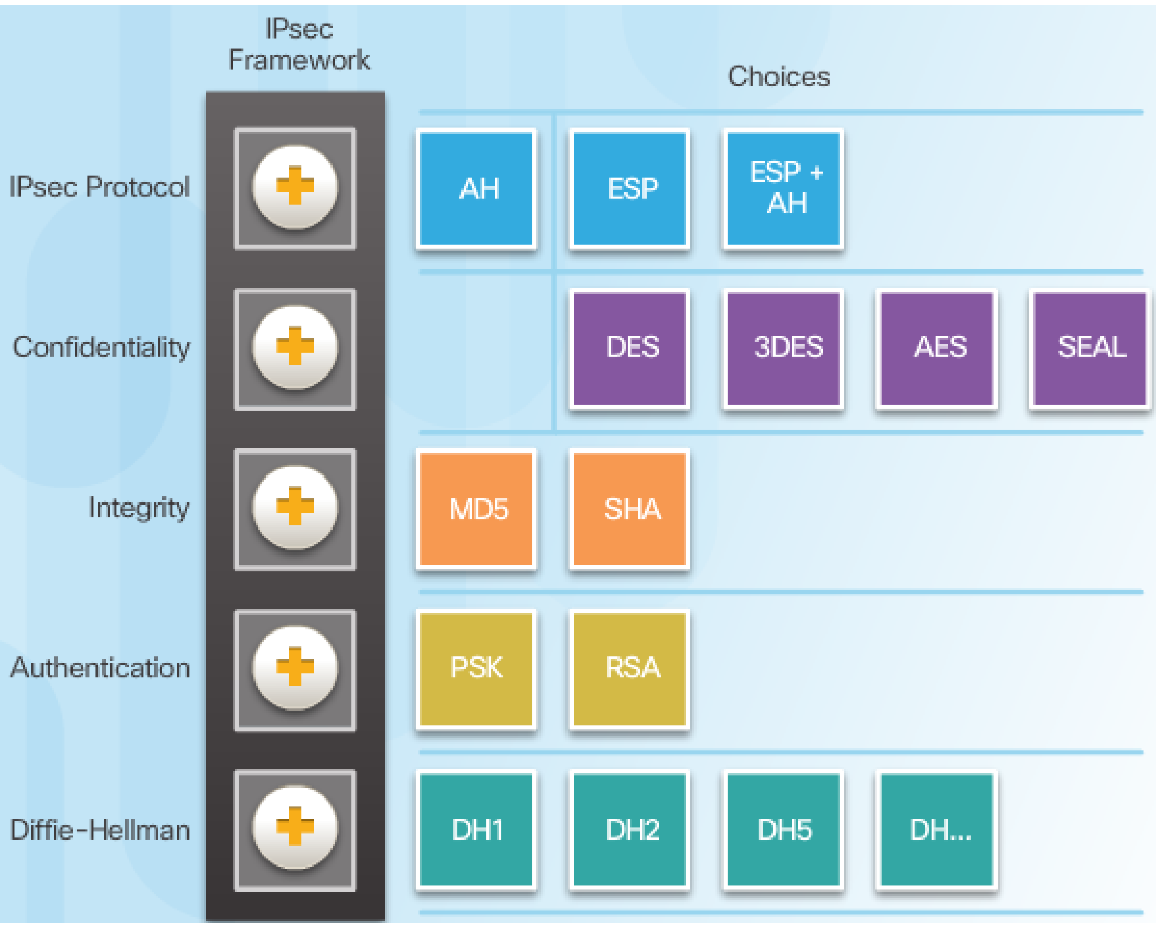
Data Integrity (Hashing) – verify that data has not been changed while in transit, if tampering is detected, the packet is dropped

Authentication (Key, Password) – verify the identity of the source of the data that is sent, ensures that the **connection** is made **with the desired communication partner**, IPsec uses Internet **Key Exchange (IKE) to authenticate users and devices** that can carry out communication independently.

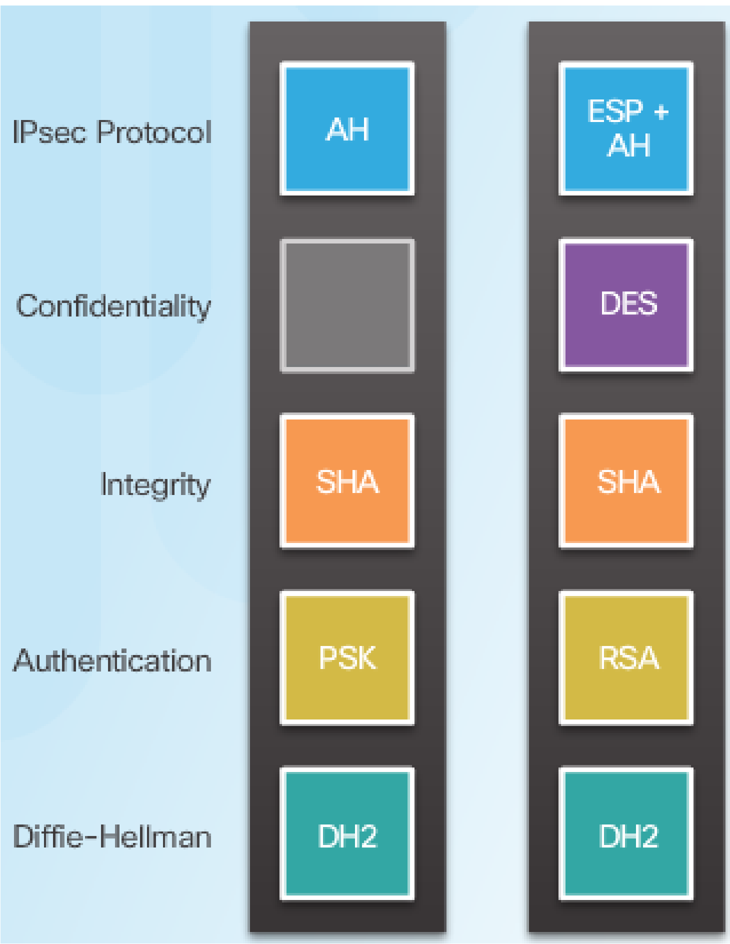
Anti-Replay Protection –
detect and reject replayed packets and helps prevent spoofing.

IPsec Technologies, Protocol Suite

IPsec Framework:

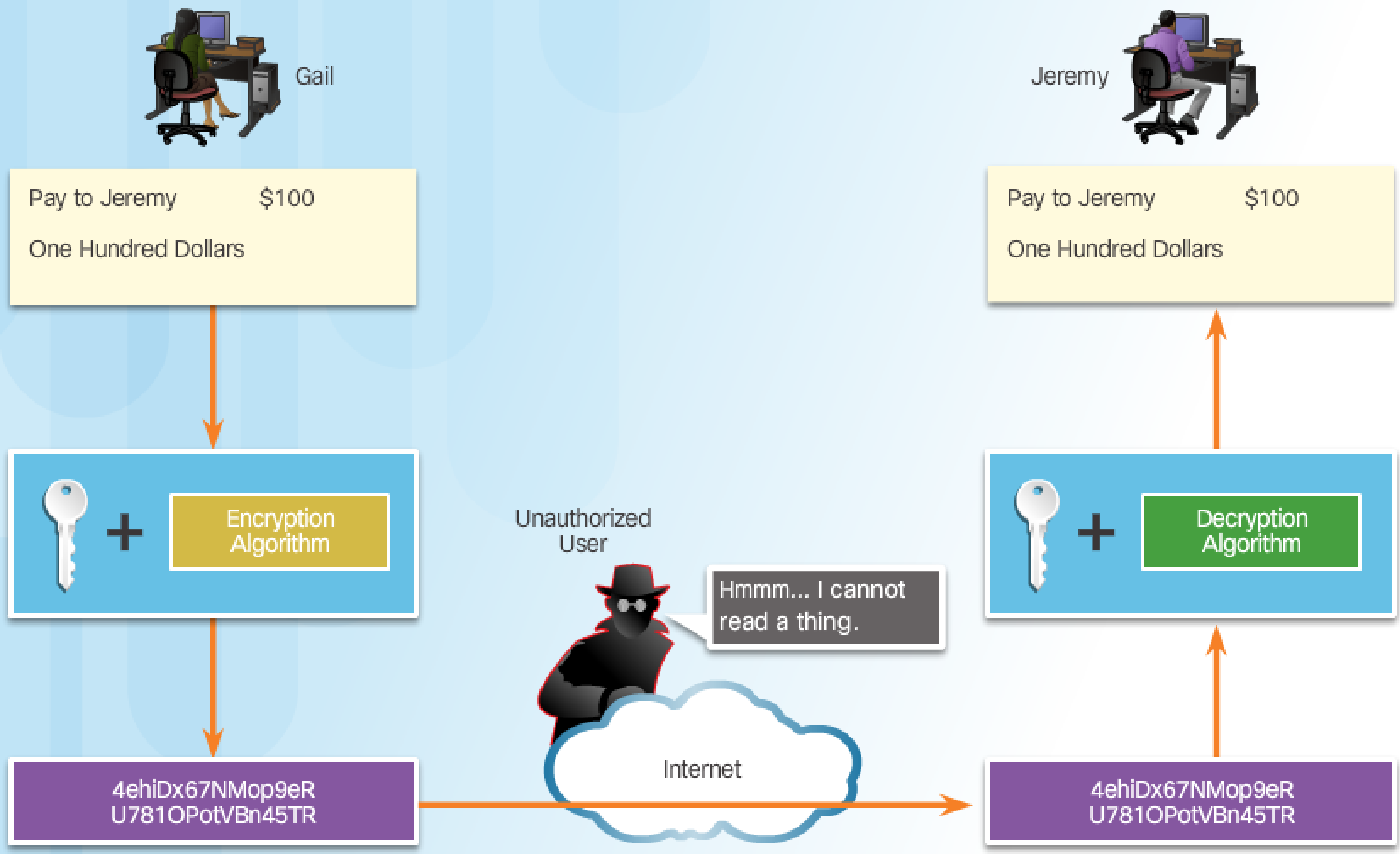


IPsec Implementation,
2 Examples:



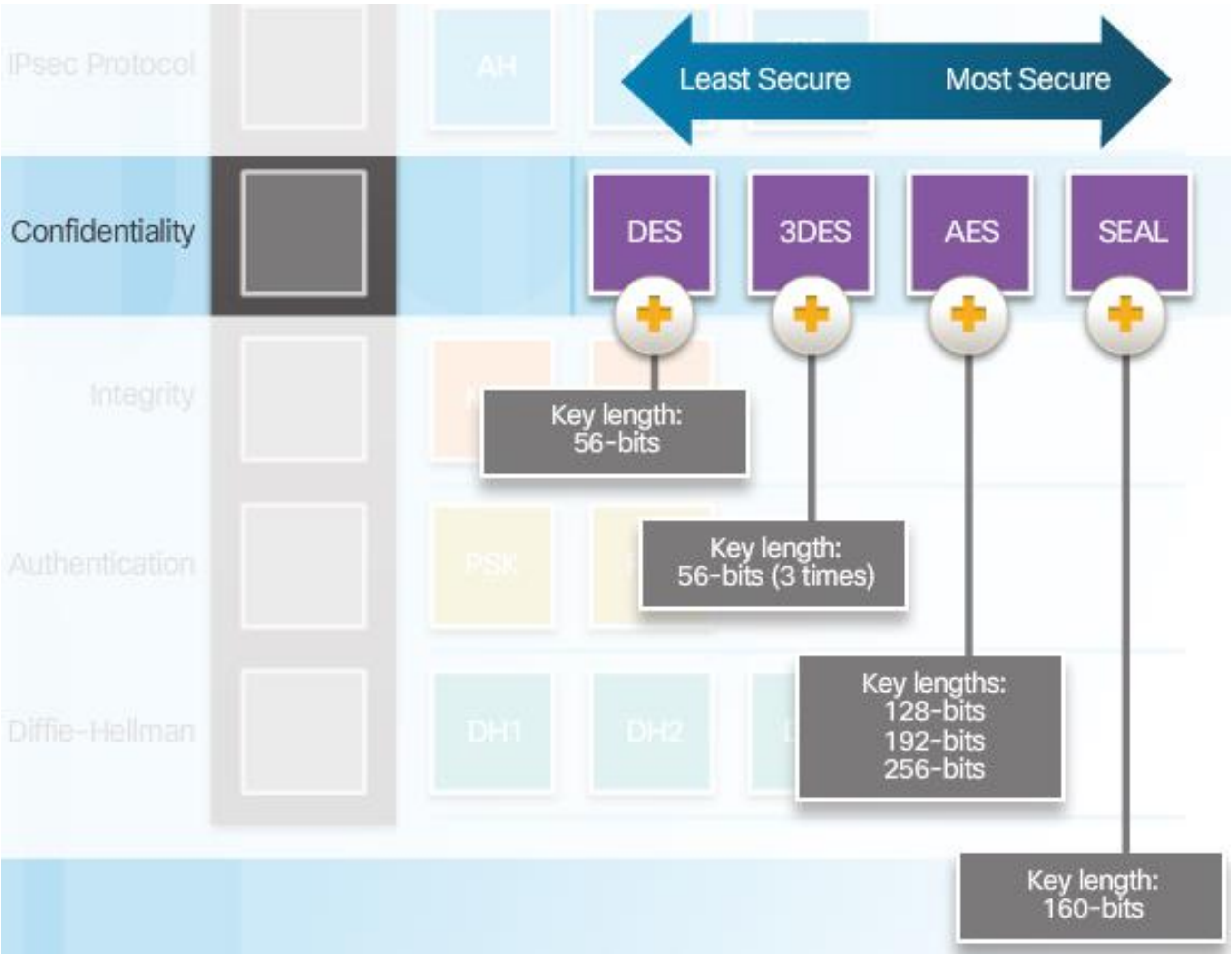
Confidentiality

Confidentiality with Encryption



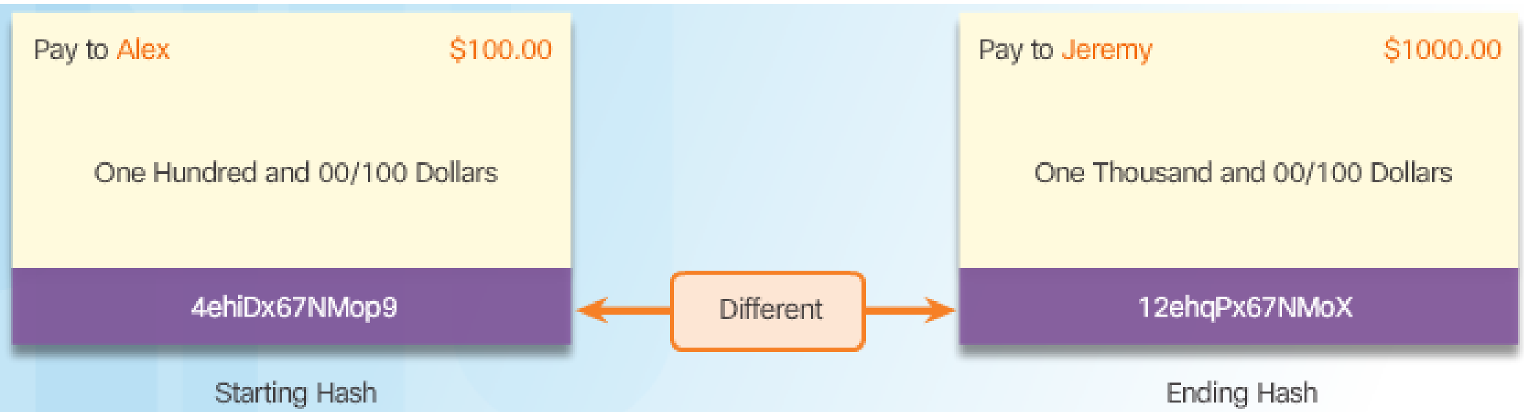
Confidentiality

Encryption Algorithms

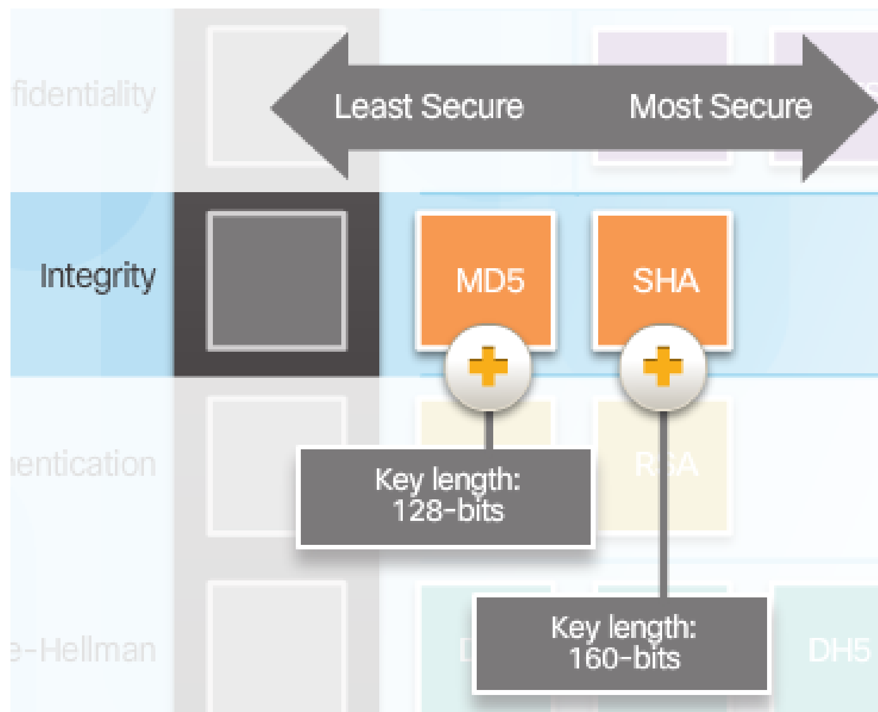


Integrity

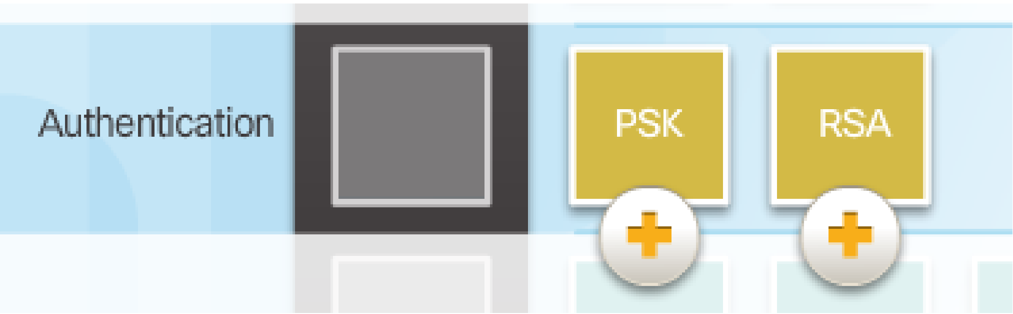
Hash Algorithms



Security of Hash Algorithms



Authentication



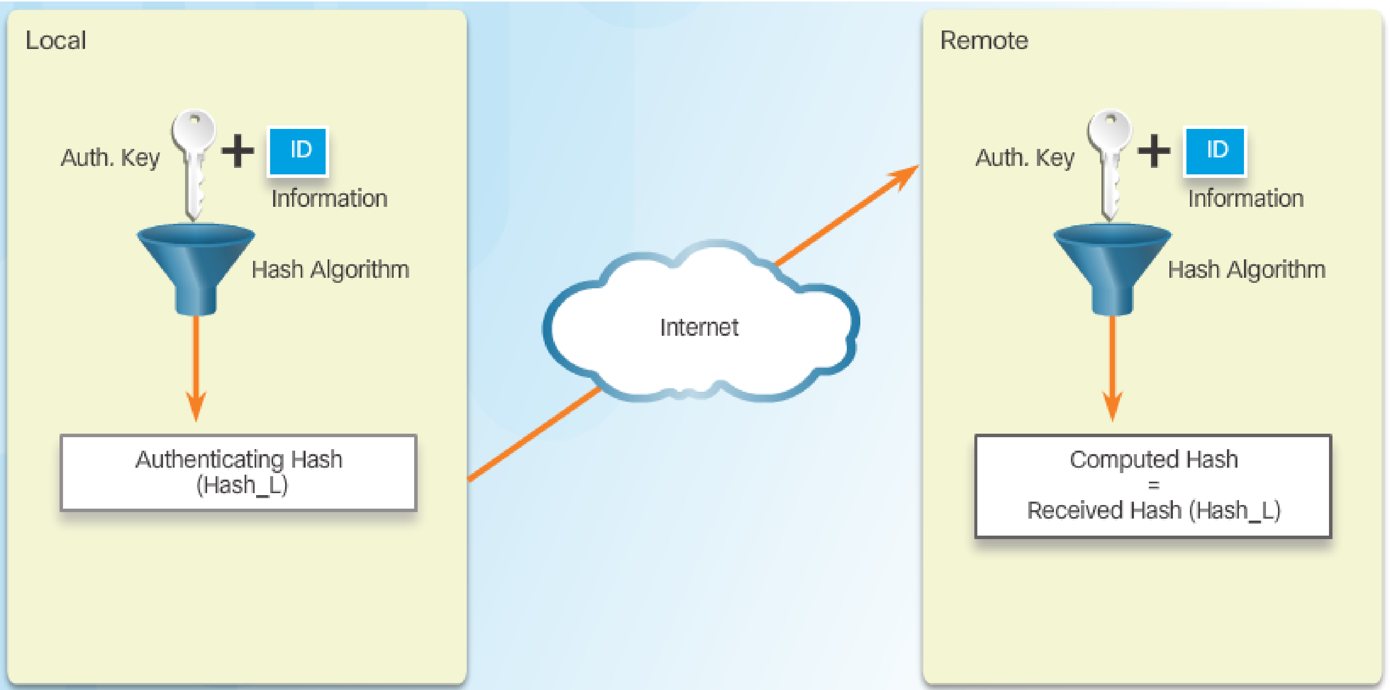
Peer Authentication Methods

PSK

A pre-shared secret key (**PSK**) value is entered into each peer **manually**.

Pre-shared keys are easy to configure manually, but do not scale well,

because each IPsec peer must be configured with the pre-shared key of every other peer with which it communicates.



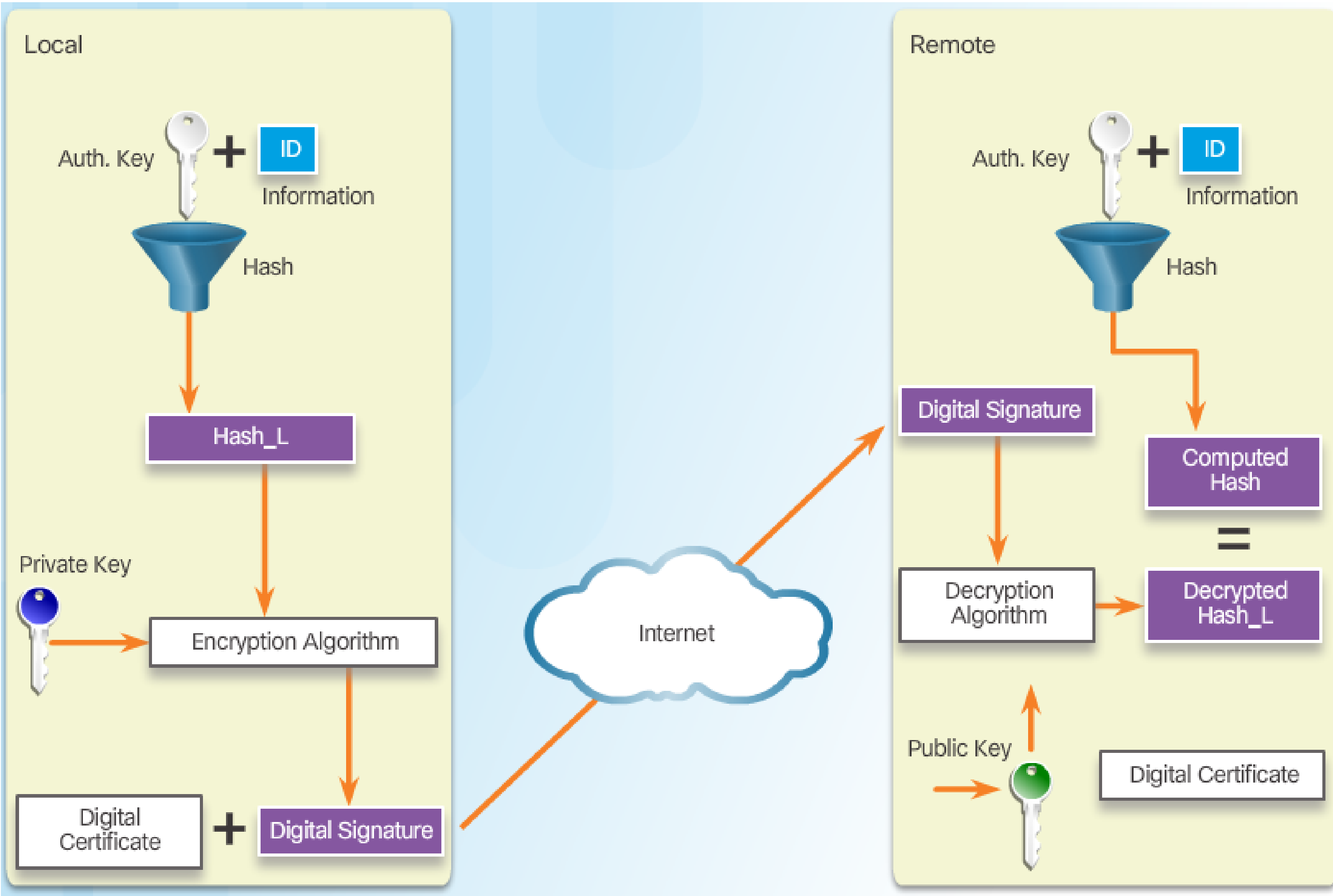
Authentication

RSA (Rivest, Shamir und Adleman) = encrypted hash + digital signature

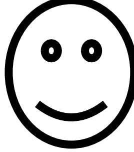
The exchange of digital certificates authenticates the peers. Each peer must authenticate its opposite peer before the tunnel is considered secure.

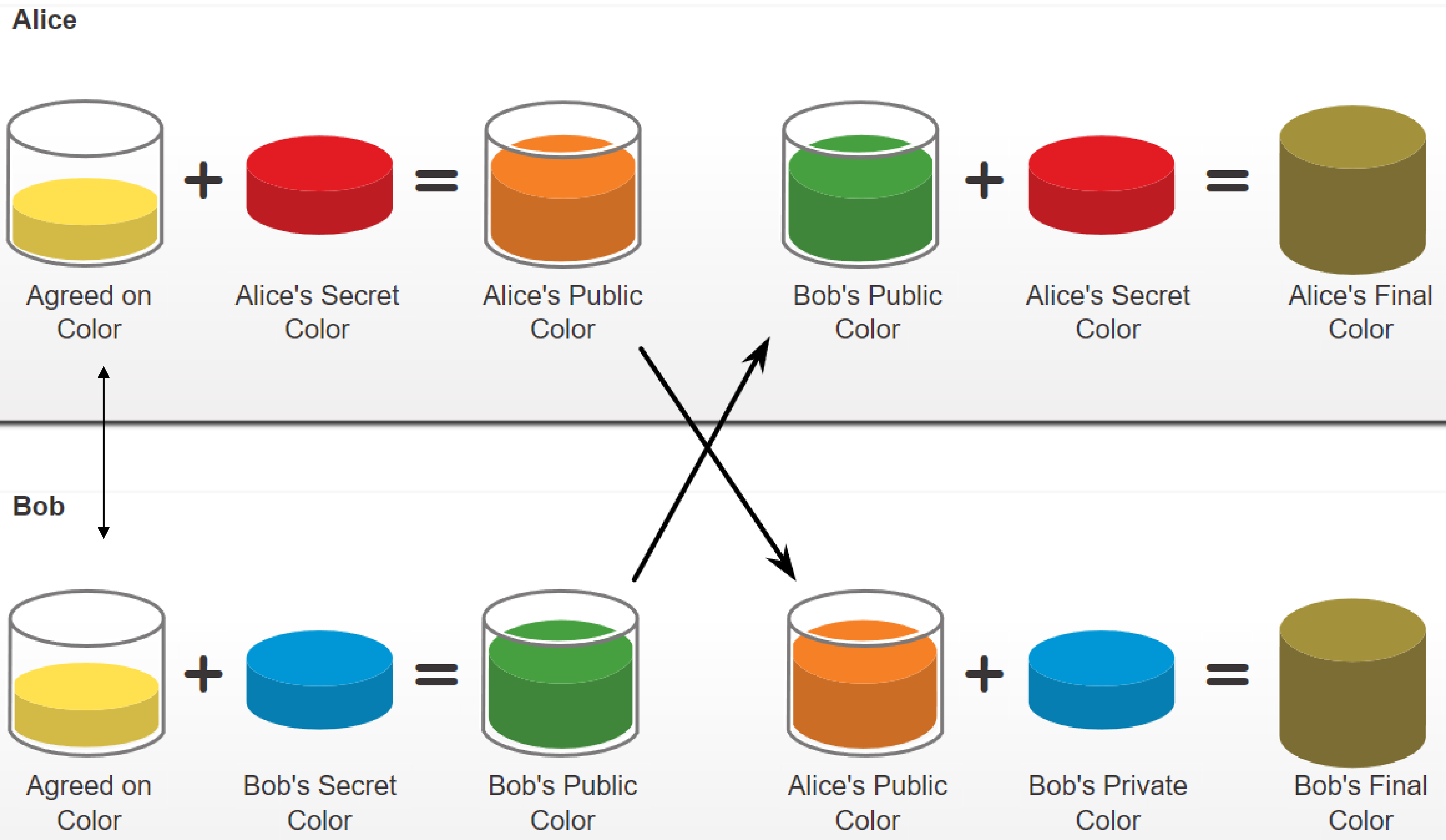
The local device derives a hash and encrypts it with its private key.
The encrypted hash is attached to the message and is forwarded to the remote end and acts like a signature.

At the remote end, the encrypted hash is decrypted using the public key of the local end. If the decrypted hash matches the recomputed hash, the signature is genuine.

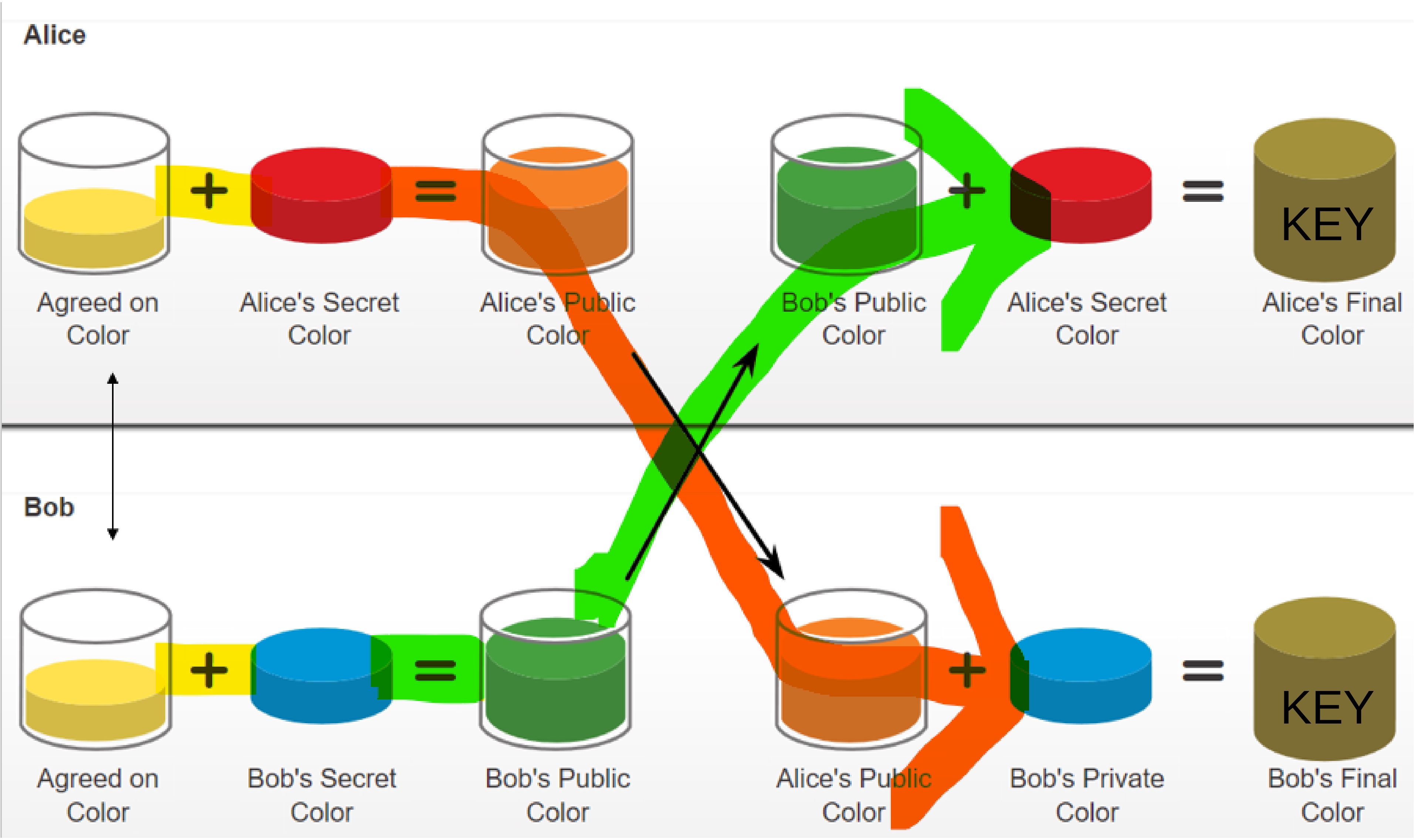


Secure Diffie-Hellman Key Exchange

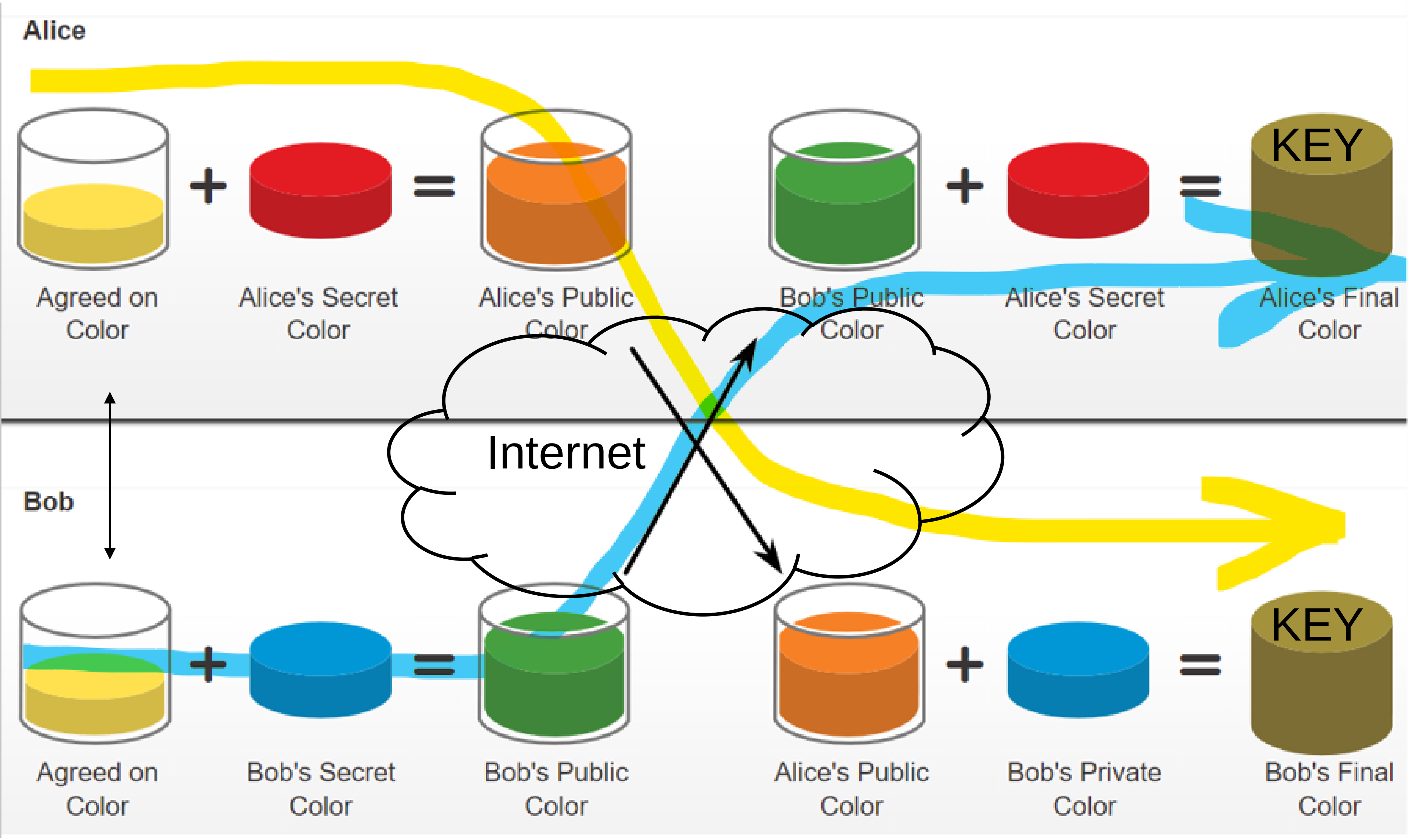




Secure Diffie-Hellman Key Exchange



Secure Diffie-Hellman Key Exchange



Secure Diffie-Hellman Key Exchange

Frage: Wie können 2 Personen sicher Daten austauschen,
ohne vorher Schlüssel transportieren zu müssen?

Antwort von Diffie und Hellmann (1976):
Indem man keine Schlüssel transportiert!

Alice will einen gemeinsamen Schlüssel K
mit Bob vereinbaren.

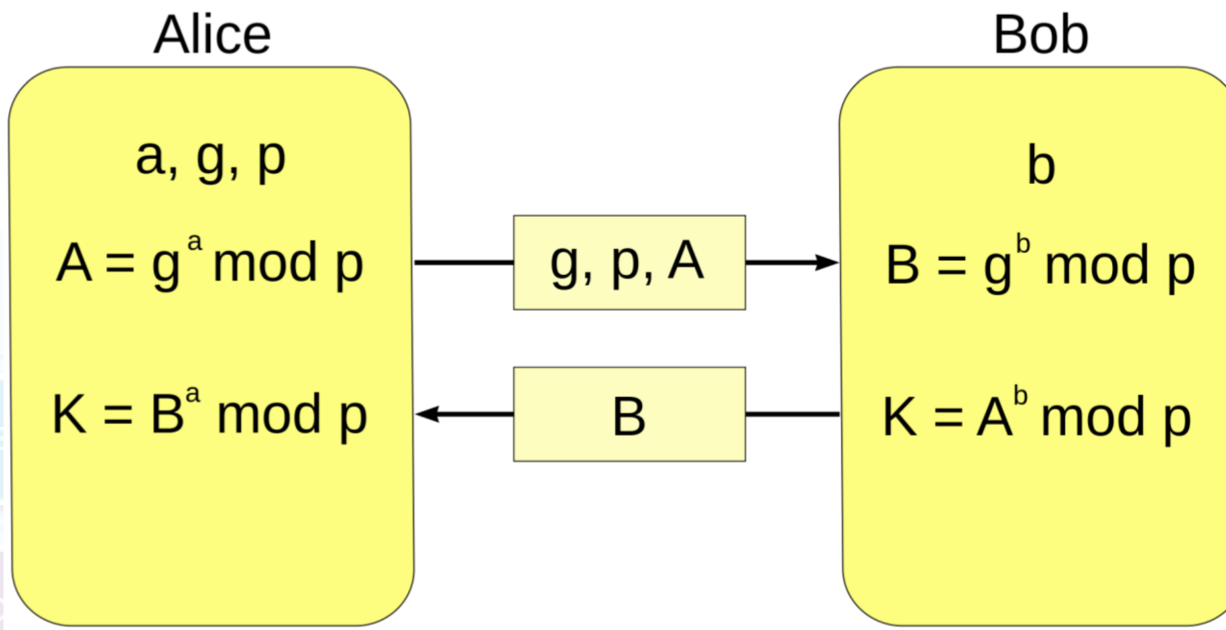
a: privater Schlüssel von Alice
b: privater Schlüssel von Bob

p: öffentlich bekannte Primzahl
g: öffentlich bekannte natürliche Zahl kleiner als p

A: öffentlicher Schlüssel von Alice
B: öffentlicher Schlüssel von Bob

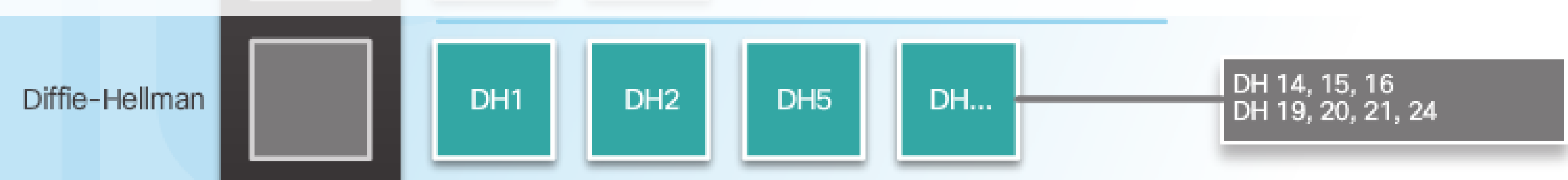
K: geheimer Sitzungs-Schlüssel für Alice und Bob

Beide errechnen einen gemeinsamen Schlüssel K, ohne dass
- a (privater Schlüssel von Alice) übertragen wurde
- b (privater Schlüssel von Alice) übertragen wurde
- K (geheimer Sitzungs-Schlüssel) übertragen wurde



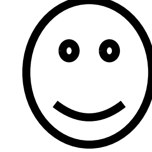
$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Diffie-Hellman group 1 - 768 bit modulus - AVOID
Diffie-Hellman group 2 - 1024 bit modulus - AVOID
Diffie-Hellman group 5 - 1536 bit modulus - AVOID
Diffie-Hellman group 14 - 2048 bit modulus – MINIMUM ACCEPTABLE
Diffie-Hellman group 19 - 256 bit elliptic curve – ACCEPTABLE
Diffie-Hellman group 20 - 384 bit elliptic curve – Next Generation Encryption
Diffie-Hellman group 21 - 521 bit elliptic curve – Next Generation Encryption
Diffie-Hellman group 24 - modular exponentiation group with a 2048-bit modulus and 256-bit prime order subgroup – Next Generation Encryption



Secure Diffie-Hellman Key Exchange

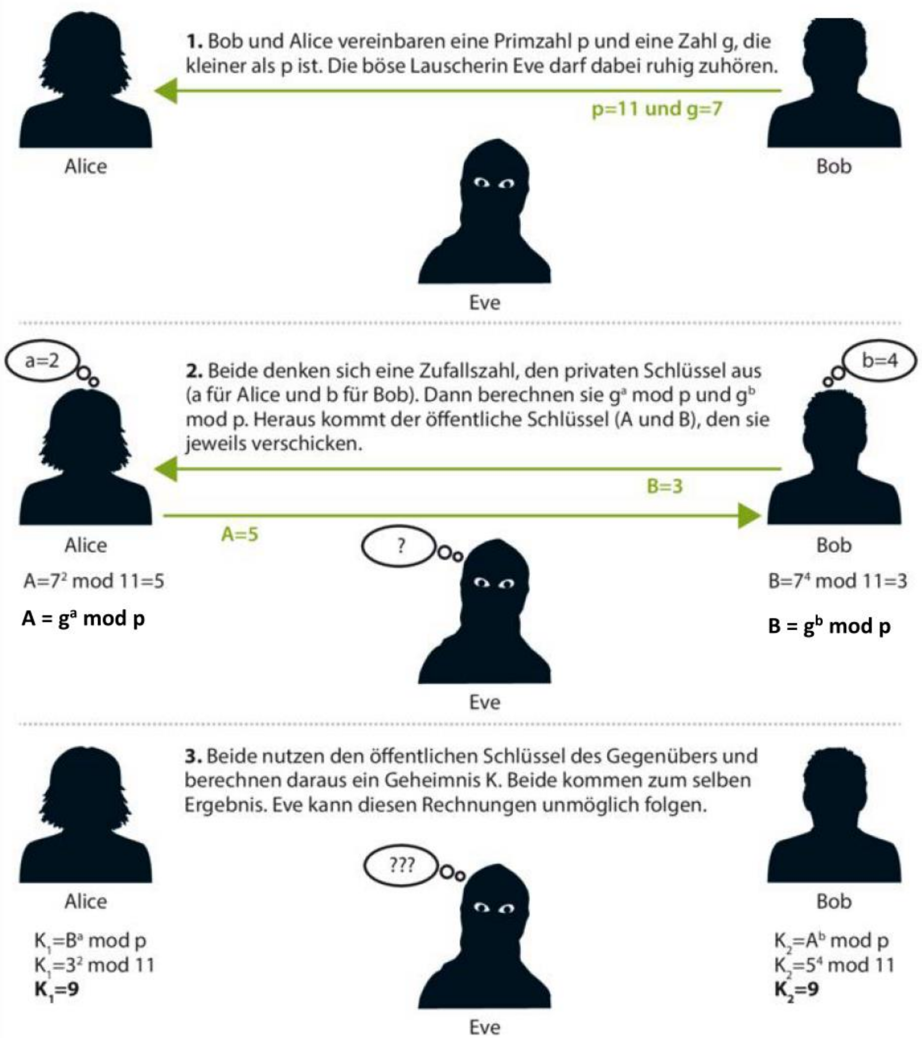
Sicherer Kanal, Symmetrische und asymmetrische Verschlüsselung, https://www.heise.de/select/ct/2021/7/2031717381985388403



Diffie-Hellman-Schlüsselaustausch

Um ein gemeinsames Geheimnis für weitere Verschlüsselung auszuhandeln, führen Alice und Bob einen Schlüsselaustausch nach Diffie und Hellman aus. Die Leitung, über die sie kommunizieren, ist ungeschützt, sodass die Lauscherin Eve zuhören kann. Aus den übermittelten Daten kann sie aber nicht auf das gemeinsame Geheimnis schließen.

SWH: g < p: stimmt nicht! Wieso?
g sollte auch eine Primzahl sein, zumindest kein Vielfaches von p.



$$A = g^a \mod p$$

Für die Beispielwerte also:

$$B = g^b \mod p$$

$$A = 7^2 \mod 11 \quad \Rightarrow \quad A = 5$$

Diesen Wert A schickt sie Bob. Der generiert sich zunächst einen öffentlichen Schlüssel (B) mit derselben Formel und schickt ihn an Alice:

$$B = 7^4 \mod 11 \quad \Rightarrow \quad B = 3$$

Jetzt folgt der wahre Kern des Verfahrens: Beide Partner setzen die erhaltenen öffentlichen Schlüssel des anderen in eine Gleichung ein, um den gemeinsamen Schlüssel K zu erhalten. Alice nimmt die Gleichung:

$$K_A = B^a \mod p$$

Und Bob äquivalent:

$$K_B = A^b \mod p$$

Beide nutzen also den öffentlichen Schlüssel des Gegenübers und als Exponenten ihren eigenen privaten Schlüssel.

Heraus kommt für Alice:

$$K_A = 3^2 \mod 11 \quad \Rightarrow \quad K_A = 9$$

Und für Bob:

$$K_B = 5^4 \mod 11 \quad \Rightarrow \quad K_B = 9$$

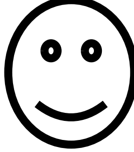
Übung: Vereinbaren Sie einen geheimen Schlüssel, ohne diesen zu übertragen.

Vereinbaren Sie mit ihrem Partner einen geheimen Schlüssel.
Vereinbaren Sie eine PZ p und eine GZ g.

Primzahlabstimmung Antwortformat: Team-Namen/ Primzahl p (>40)/ Ganze Zahl g (auch Primzahl, kein Vielfaches von p).

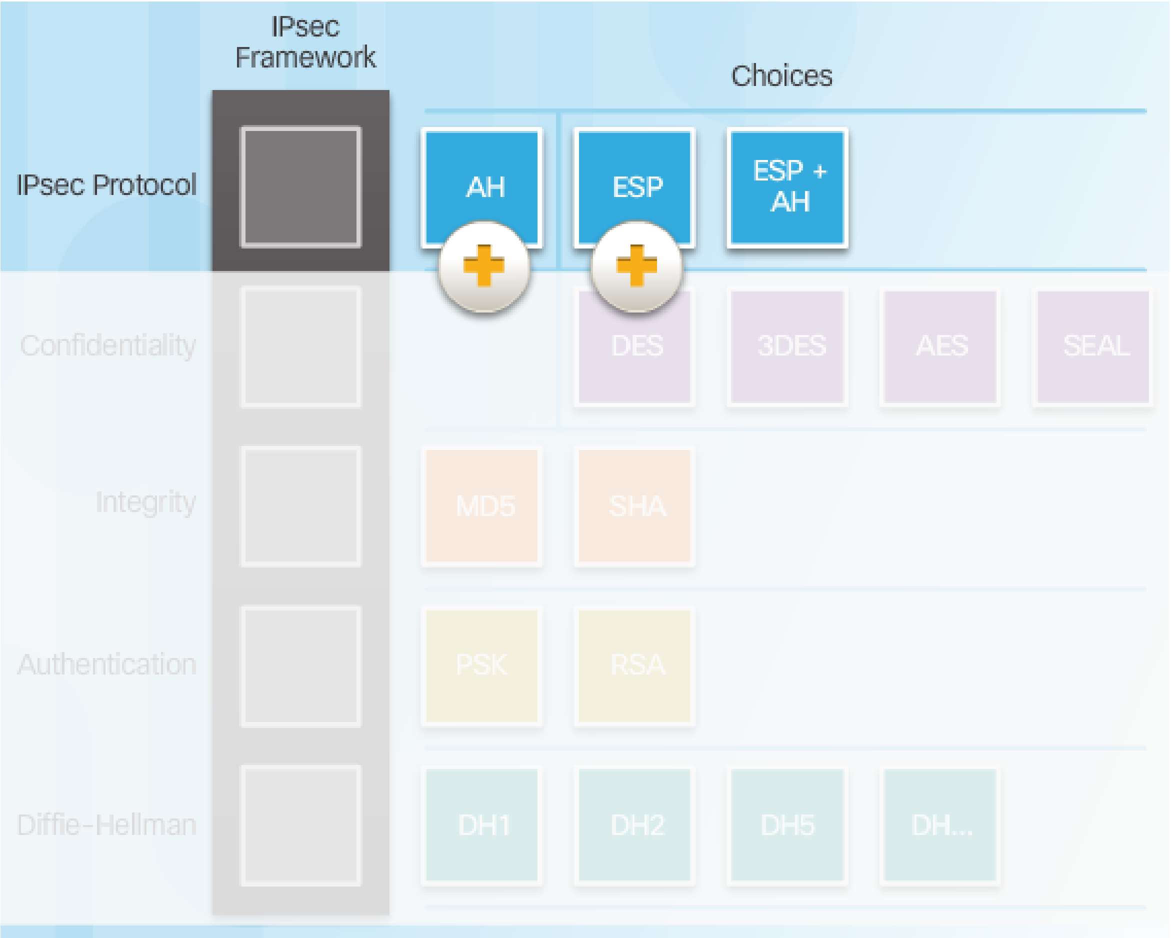
	p	g	a	b	A	B	**KA**	**KB**
	17	3	3	7	10	11	**5**	**5**
					=MOD(C5^D5;B5)	=MOD(C5^E5;B5)	=MOD(G5^D5;B5)	=MOD(F5^E5;B5)

IPsec Protocol Overview

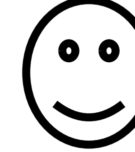


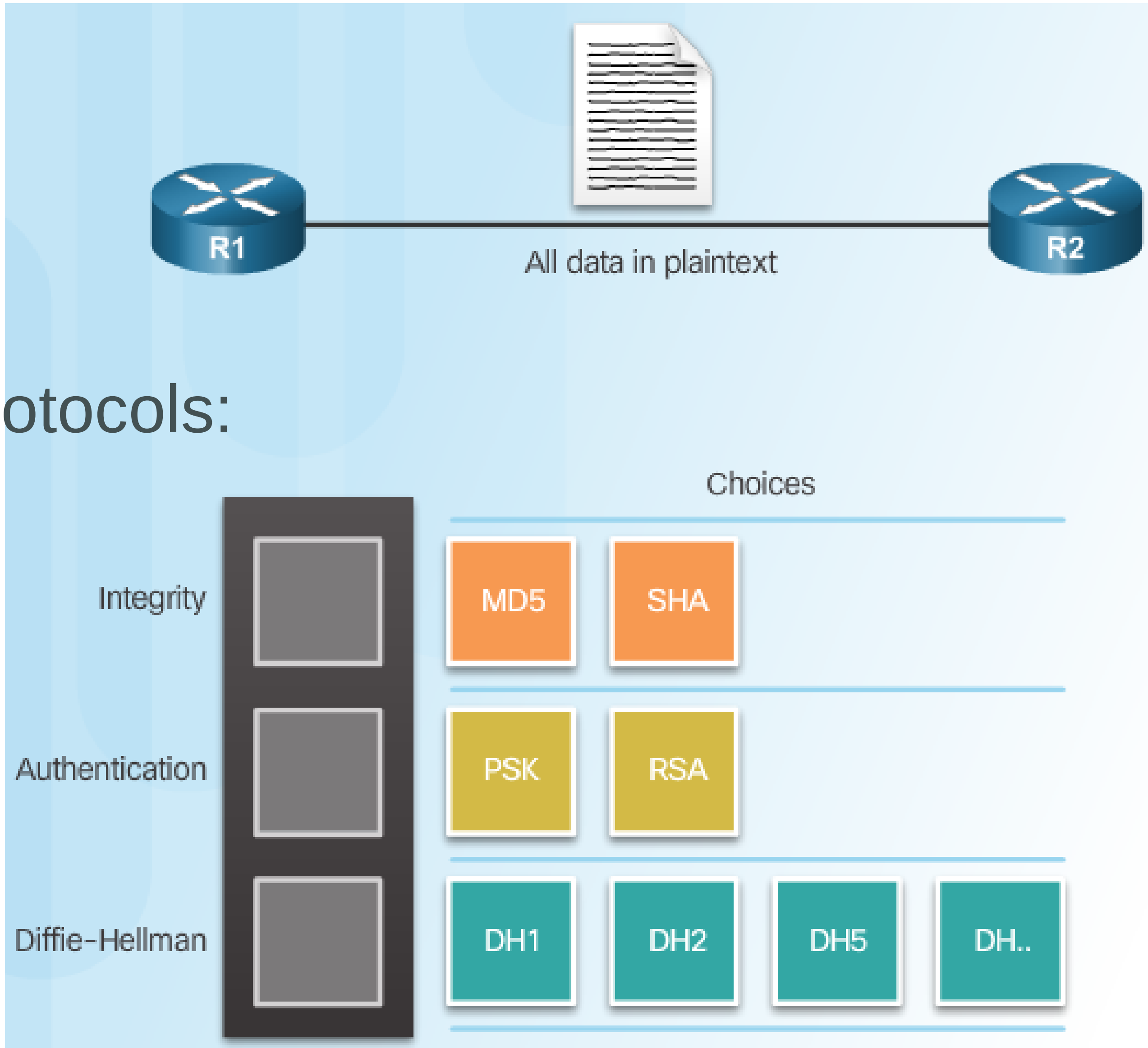
Authentication Header (AH)
AH provides only data integrity and data authentication.

Encapsulating Security Payload (ESP)
ESP provides **confidentiality**, data integrity and data authentication.



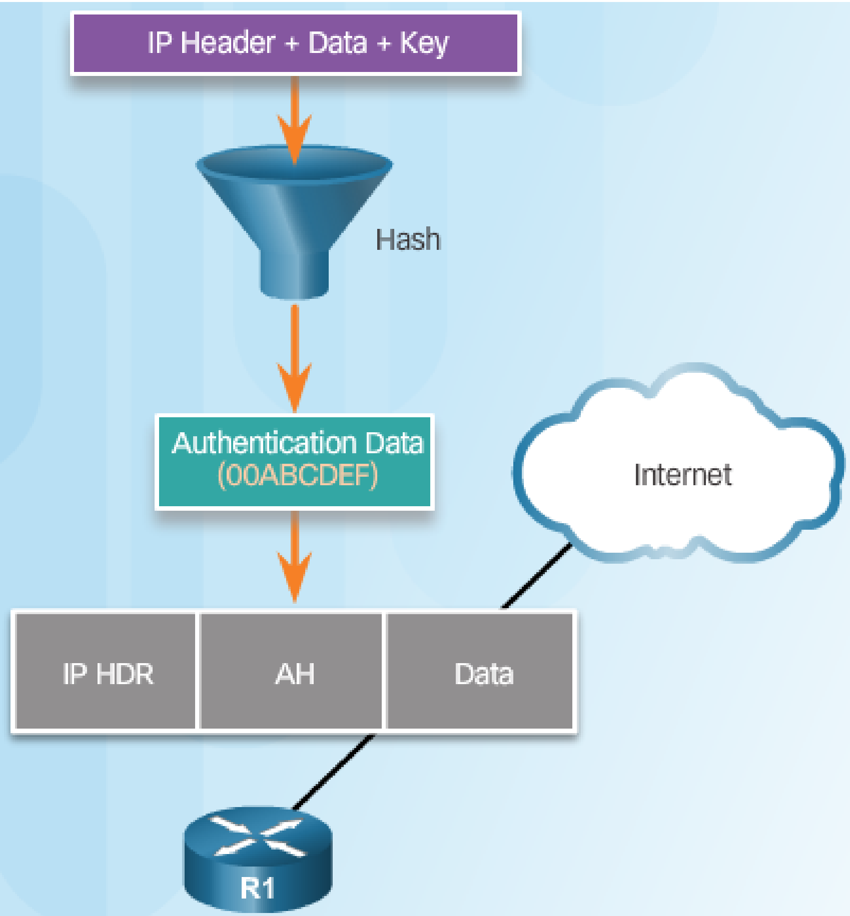
Authentication Header (AH)



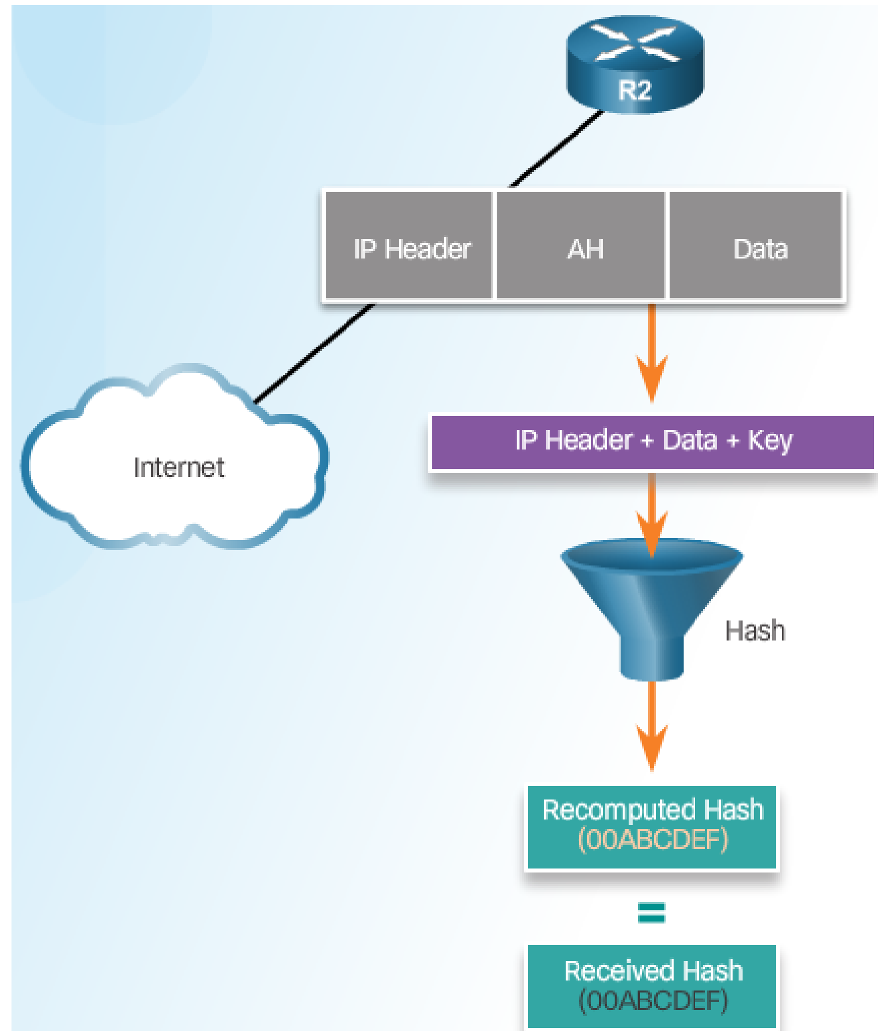


AH Protocols:

Authentication Header (AH)

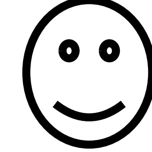


Router **Creates Hash** and **Transmits** to Peer

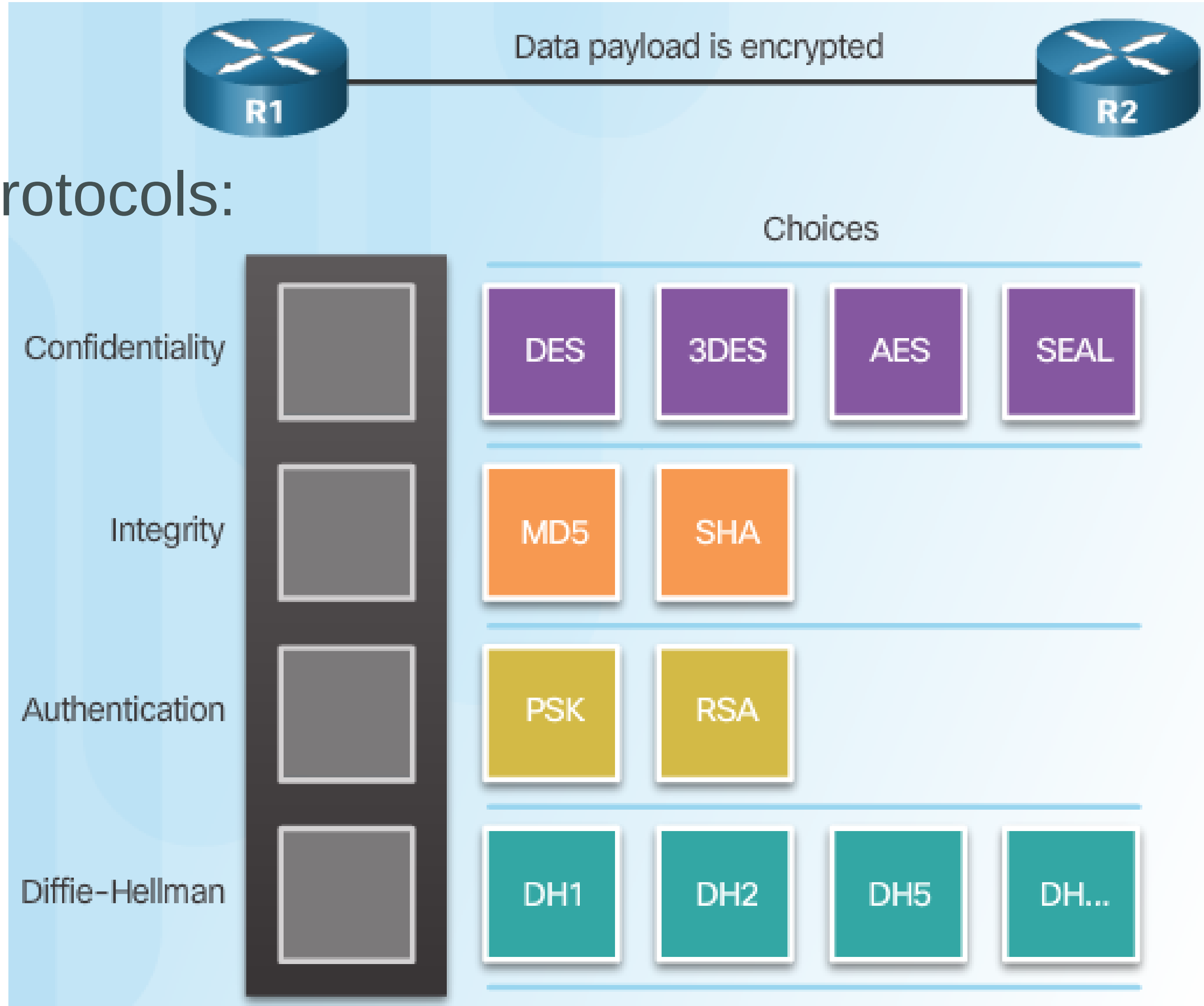


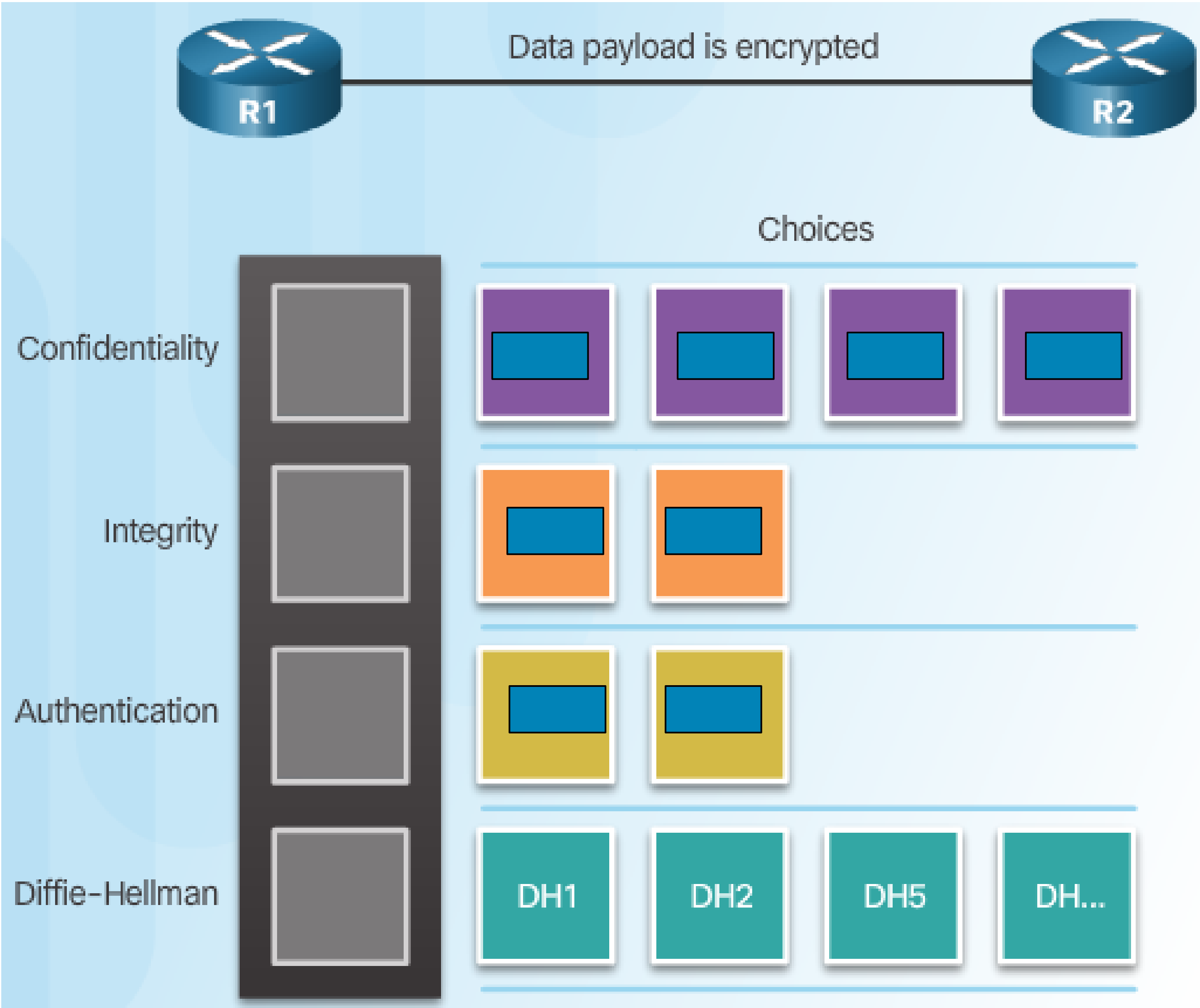
Peer Router **Compares Recomputed Hash to Received Hash**

Encapsulating Security Payload (ESP)

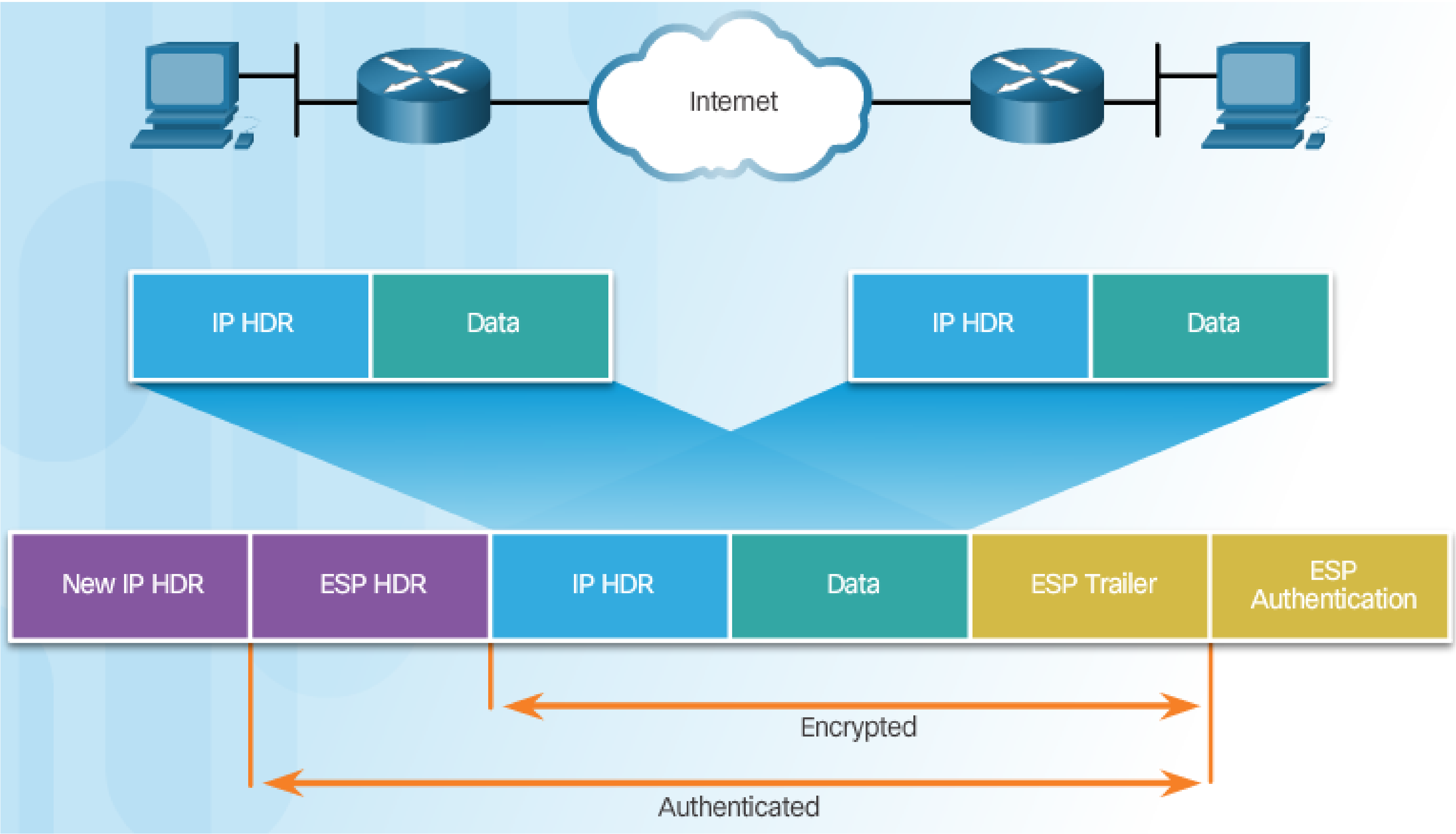


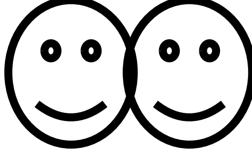
ESP Protocols:




R1
Data payload is encrypted
R2
Choices
Confidentiality
Integrity
Authentication
Diffie-Hellman
DH1
DH2
DH5
DH...

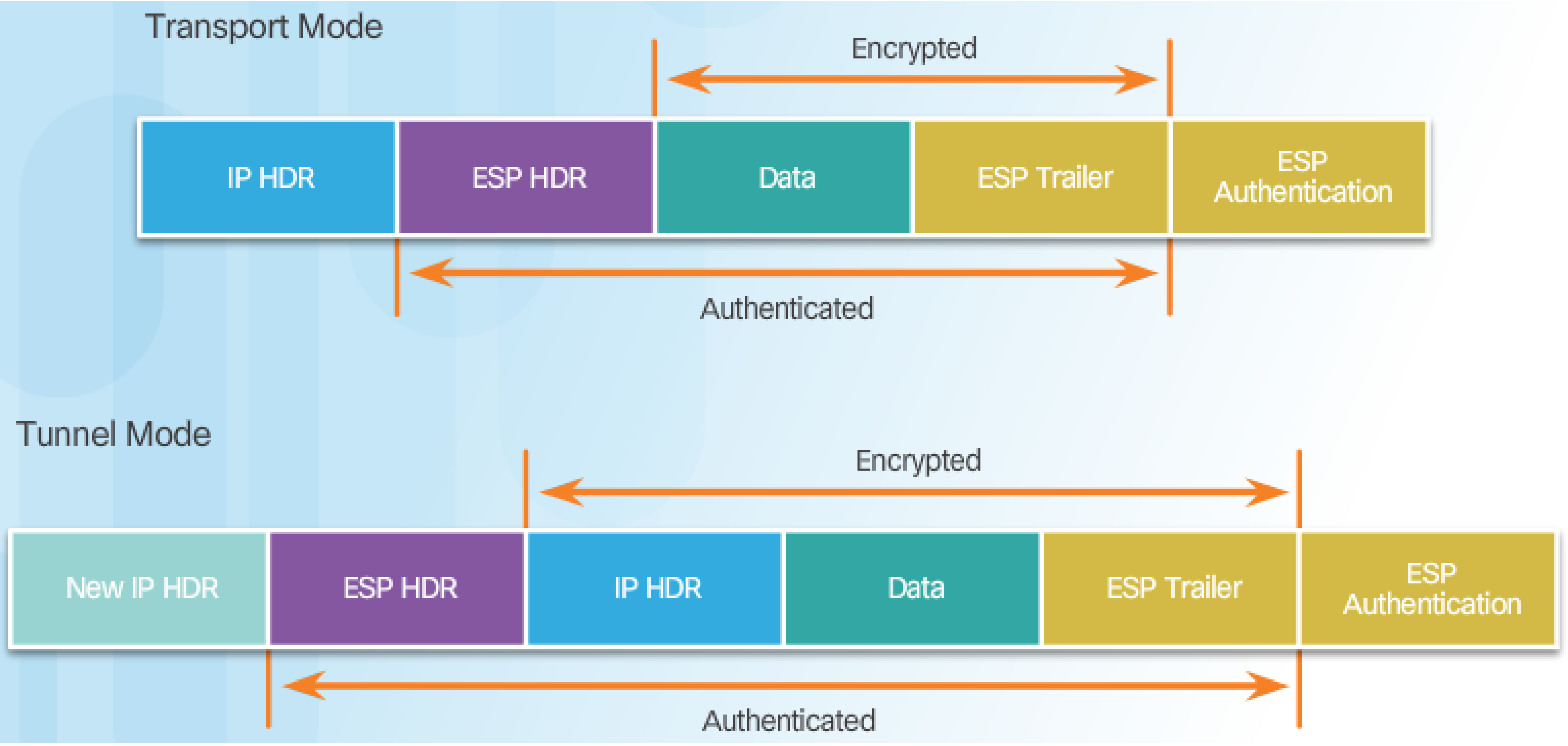
ESP Encrypts and Authenticates





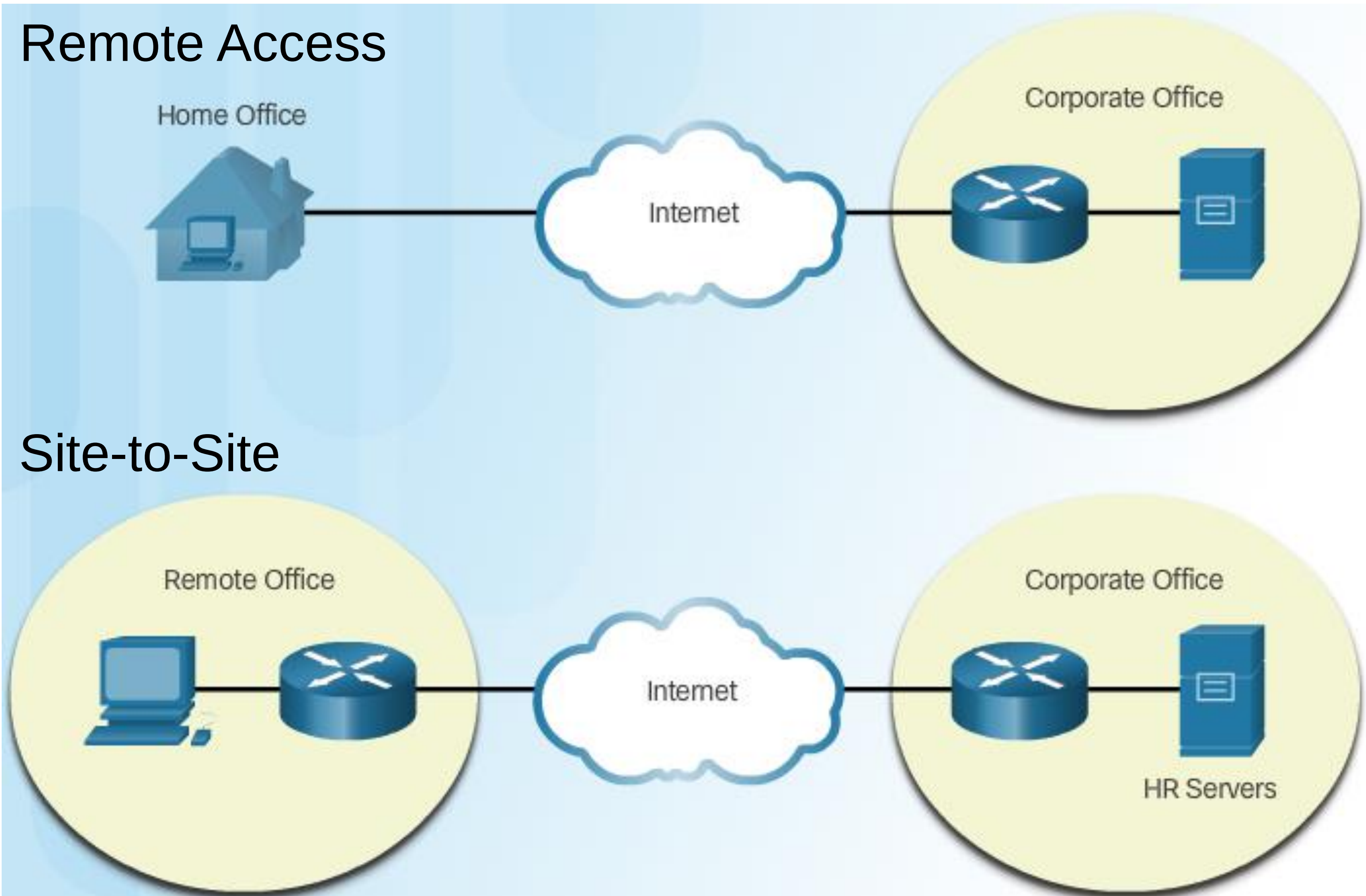
Transport and Tunnel Modes

Apply AH and ESP in Two Modes



Transport and Tunnel Modes

IPsec deployments



Glossary

- DES - Data Encryption Standard
- AES - Advanced Encryption Standard
- SEAL - Software-Optimized Encryption Algorithm

- SHA - Secure Hash Algorithm
- MD5 - Message-Digest Algorithm 5 = Hash Algorithm
- HMAC – Keyed - **H**ash **M**essage **Authentication** **C**ode
  (HMAC_MD5, HMAC_SHA1, HMAC_SHA256, etc.)

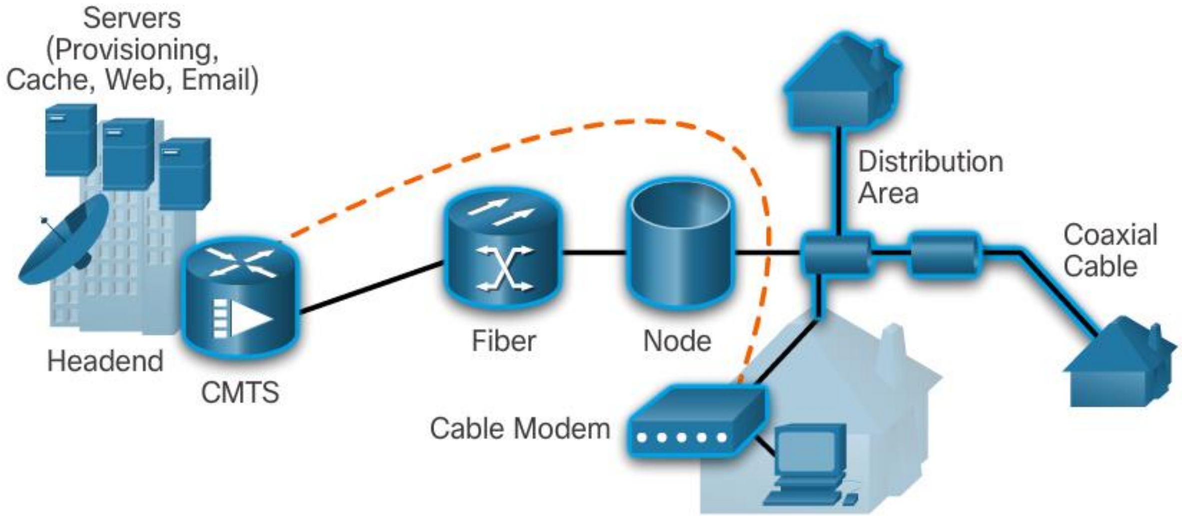
- RSA - Rivest, Shamir und Adleman
- PSK - Pre-Shared Key

- AH - Authentication Header
- ESP - Encapsulating Security Payload

Access Connections

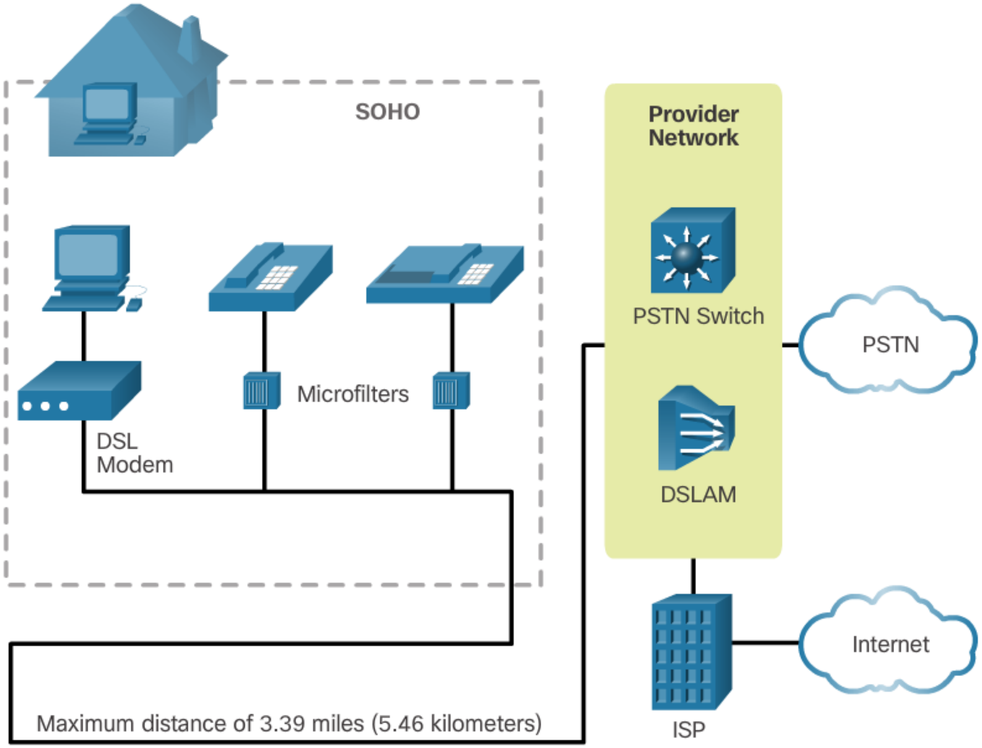
Broadband Connections - Cable TV System

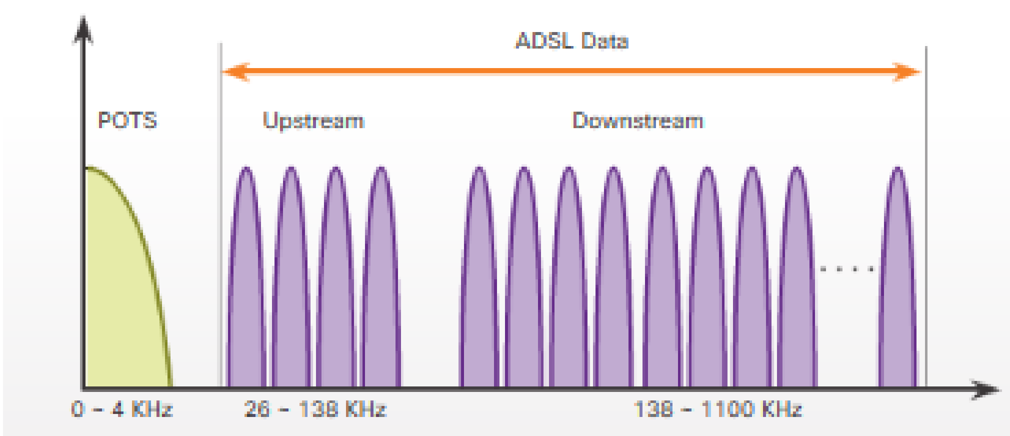
- The **cable TV system** uses a **coaxial cable** that carries radio frequency (RF) signals across the network.
- A **headend CMTS (Cable Modem Termination System)** communicates with CMs located in subscriber homes.
- **The HFC (Hybrid Fiber Coax) network** is a mixed optical-coaxial network in which **optical fiber replaces the lower bandwidth coaxial cable**.



Broadband Connections - DSL

- A Digital Subscriber Line (DSL) is a means of providing high-speed connections **over installed copper wires**.
- The two important components are the **DSL transceiver (modem)** and the **DSLAM** (DSL access multiplexer)**.**
- The advantage that DSL has over cable technology is that **each user has a separate direct connection** to the DSLAM.
- Asymmetric DSL (**ADSL**) **bandwidth allocation** on a copper wire.
  POTS (Plain Old Telephone System) identifies the frequency range used by the telephone service.

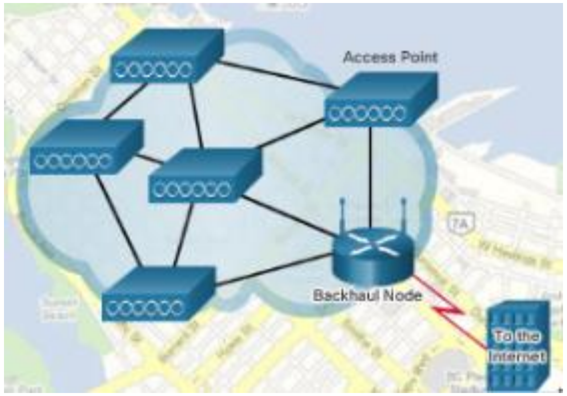


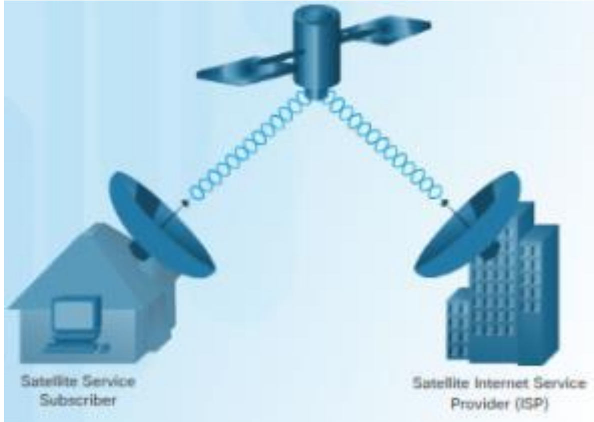


Remote Access Connections

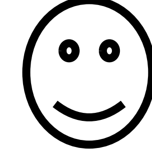
Broadband Connections - Wireless

- **Three main technologies**:
  - **Municipal Wi-Fi** - Most municipal wireless networks use a **mesh of interconnected access points**. **Each access point** is in range and **can communicate with at least two other access points**.
  - **Cellular/mobile** - Mobile phones use radio waves **to communicate through nearby cell towers**. Cellular/mobile broadband access consists of various standards.
  - **Satellite Internet** - Satellite Internet services are used in locations **where land-based Internet access is not available**, or for **temporary installations** that are mobile. Internet access using satellites is **available worldwide**.



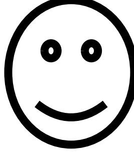


Select a Broadband Connection



- Each broadband solution has **advantages** and **disadvantages**.

- Some **factors** to consider in making a decision include:
  - **Cable** - Bandwidth is shared by many users, upstream data rates are often **slow during high-usage hours** in areas with over-subscription.
  - **DSL** - Limited bandwidth that is **distance sensitive** (in relation to the ISP’s central office), upstream rate is proportionally quite small compared to downstream rate.
  - **Fiber-to-the-Home** - Requires fiber installation directly to the home.
  - **Cellular/Mobile** - **Coverage** is often an issue, **bandwidth is not guaranteed**.
  - **Wi-Fi Mesh** - **Most municipalities do not have a mesh network deployed**; if it is available, then it is a viable option.
  - **Satellite** - **Expensive**, **limited capacity per subscriber**; provides **access where no other access is possible**.



PPPoE

PPPoE creates a **PPP tunnel over an Ethernet connection**.

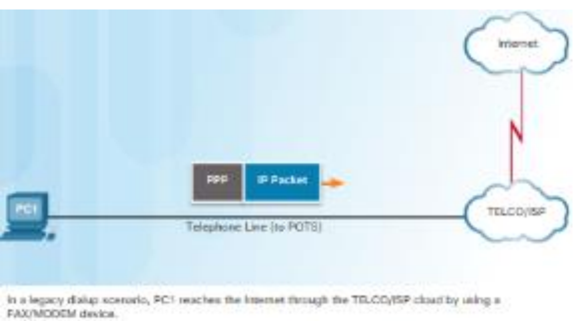
This allows **PPP frames to be sent across the Ethernet cable to the ISP from the customer’s router**.

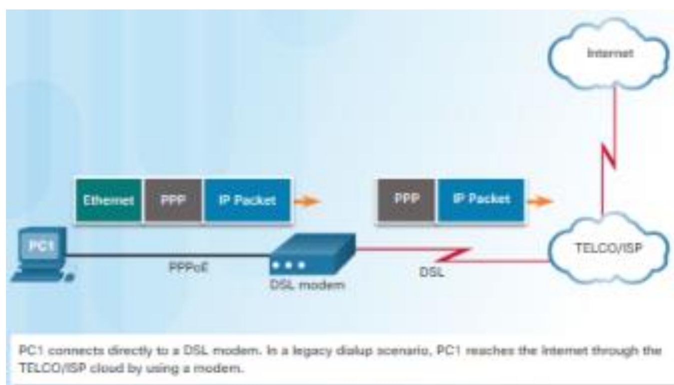
The modem converts the Ethernet frames to PPP frames by stripping the Ethernet headers. The modem then transmits these PPP frames on the ISP’s DSL network.

PPPoE Overview

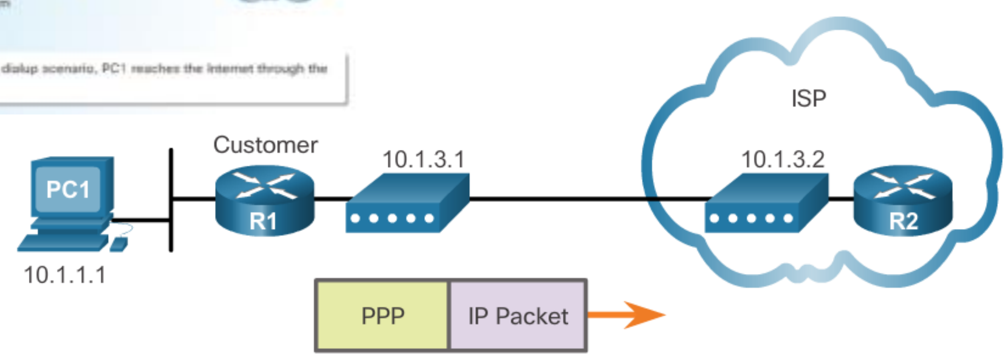
PPP can be used on **all serial links** including those links created with **dial-up analog** and **ISDN modems**.

- PPP supports the **ability to assign IP addresses to remote ends** of a PPP link.
- PPP supports **CHAP authentication**.
- **Ethernet links do not natively support PPP**.
  PPP over Ethernet (PPPoE) provides a solution to this problem.
  PPPoE creates a PPP tunnel over an Ethernet connection.



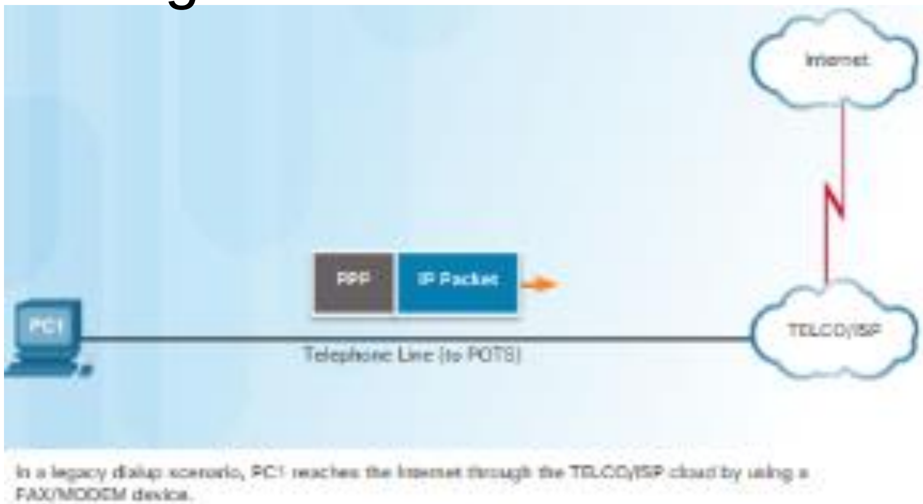


Evolution

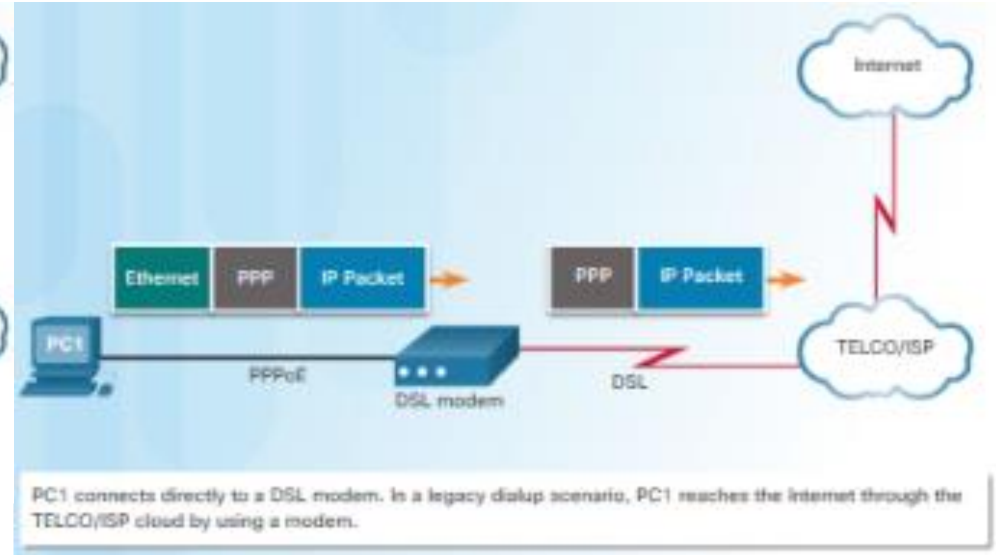


PPPoE Evolution

analogue modem

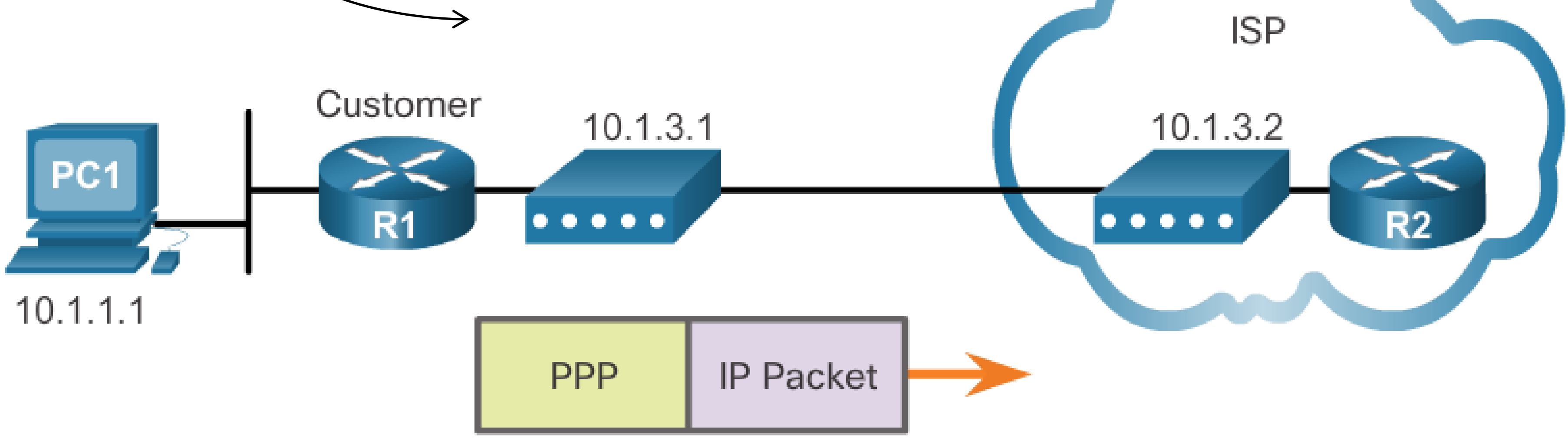


DSL modem

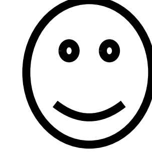


Evolution

Router + DSL modem



Implementing PPPoE



PPPoE **Configuration**

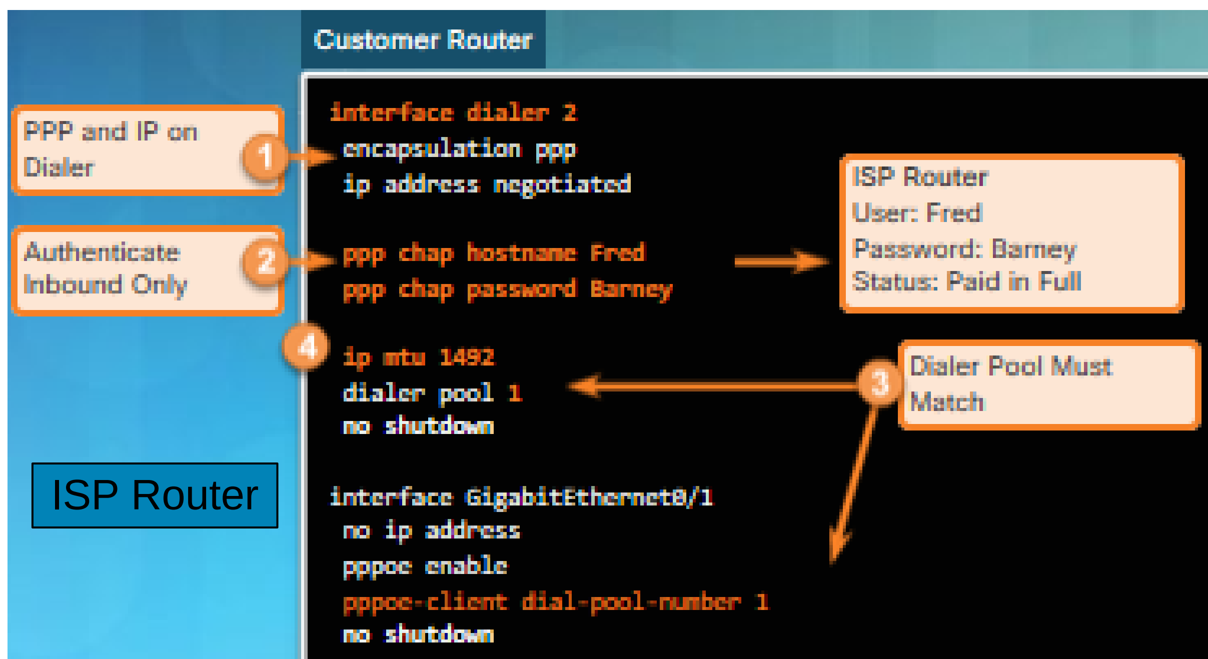
- To **create a PPP tunnel**, the configuration uses a virtual **dialer interface**.
  The dialer interface is created using the **interface dialer** *number* command.
- The PPP CHAP configuration usually defines one-way authentication; therefore, the ISP authenticates the customer.
- The physical Ethernet interface that connects to the DSL modem is then enabled with the command **pppoe enable**.
- The dialer interface is linked to the Ethernet interface with the **dialer pool** and **pppoe-client** commands, using the same number.
- The **maximum transmission unit (MTU) to be set down to 1492**, versus the default of 1500, **to accommodate the PPPoE headers**.

Customer Router

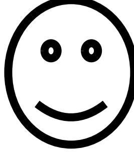
```
R1(config)# interface dialer 5
R1(config-if)# encapsulation ppp
R1(config-if)# ip address negotiated

R1(config-if)# ip mtu 1492
R1(config-if)# dialer pool 5

R1(config-if)# ppp chap hostname customer2222
R1(config-if)# ppp chap password ConnectMe
R1(config-if)# no shutdown
```

ISP Router

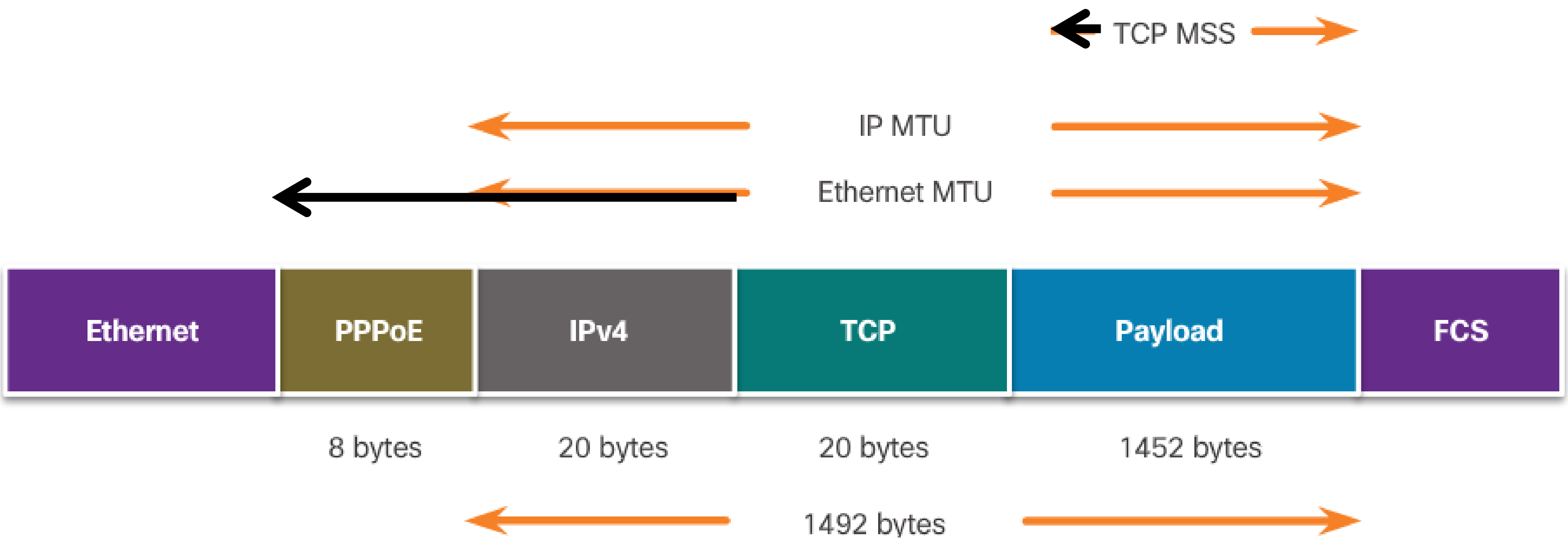
```
R1(config-if)# interface GigabitEthernet 0/0
R1(config-if)# no ip address
R1(config-if)# pppoe enable
R1(config-if)# pppoe-client dial-pool-number 5
R1(config-if)# no shutdown
```



Implement PPPoE



- Adjusting the TCP MSS value
  - **PPPoE supports an MTU (**max. transmission unit**) of only 1492 bytes** in order to accommodate the **additional 8-byte PPPoE header**. **Payload size is 1452 Byte**.
  - The **ip tcp adjust-mss 1452 (***max-segment-size)* interface command adjusts the MSS (max. segment size) value during the TCP 3-way handshake.

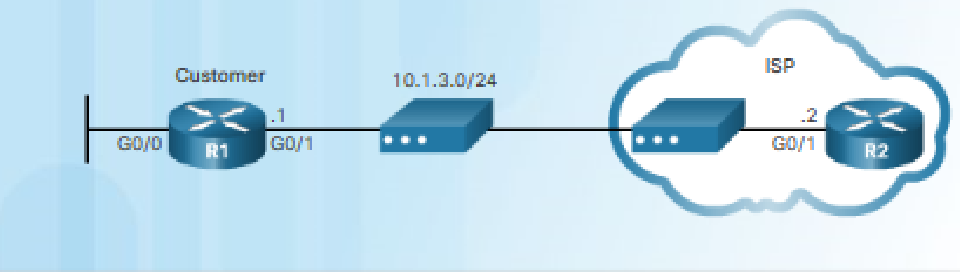


Implement PPPoE

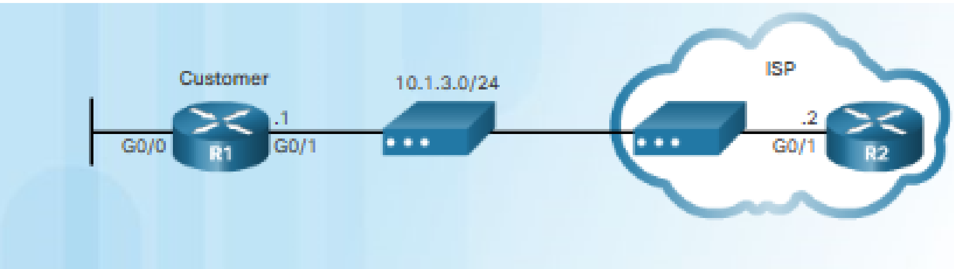
- PPPoE **Verification**
  - The **show ip interface brief** command is issued to verify the IPv4 address automatically assigned to the dialer interface by the ISP router.
  - The **show interface dialer** command verifies the MTU and PPP encapsulation configured on the dialer interface.
  - The **show pppoe session** command is used to display information about currently active PPPoE sessions.
  - The Ethernet MAC addresses can be verified by using the **show interfaces** command on each router.
- PPPoE **Troubleshooting**
  - Verify PPP negotiation using the **debug ppp negotiation** command.
  - Re-examine the output of the **debug ppp negotiation** command.

Verifying PPPoE

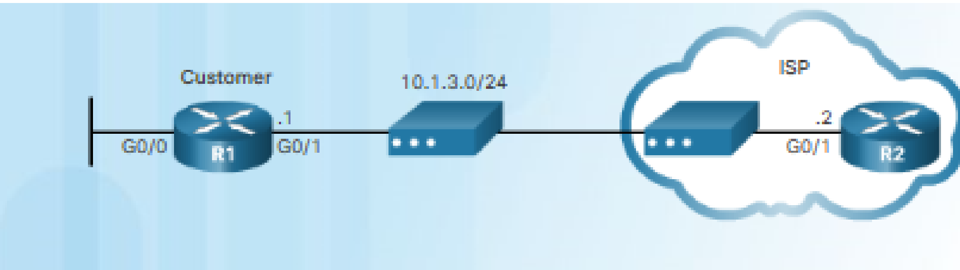

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
Dialer2                    10.1.3.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
```




```
R1# show interface dialer 2
Dialer2 is up, line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.3.1/32
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset
<output omitted>
```



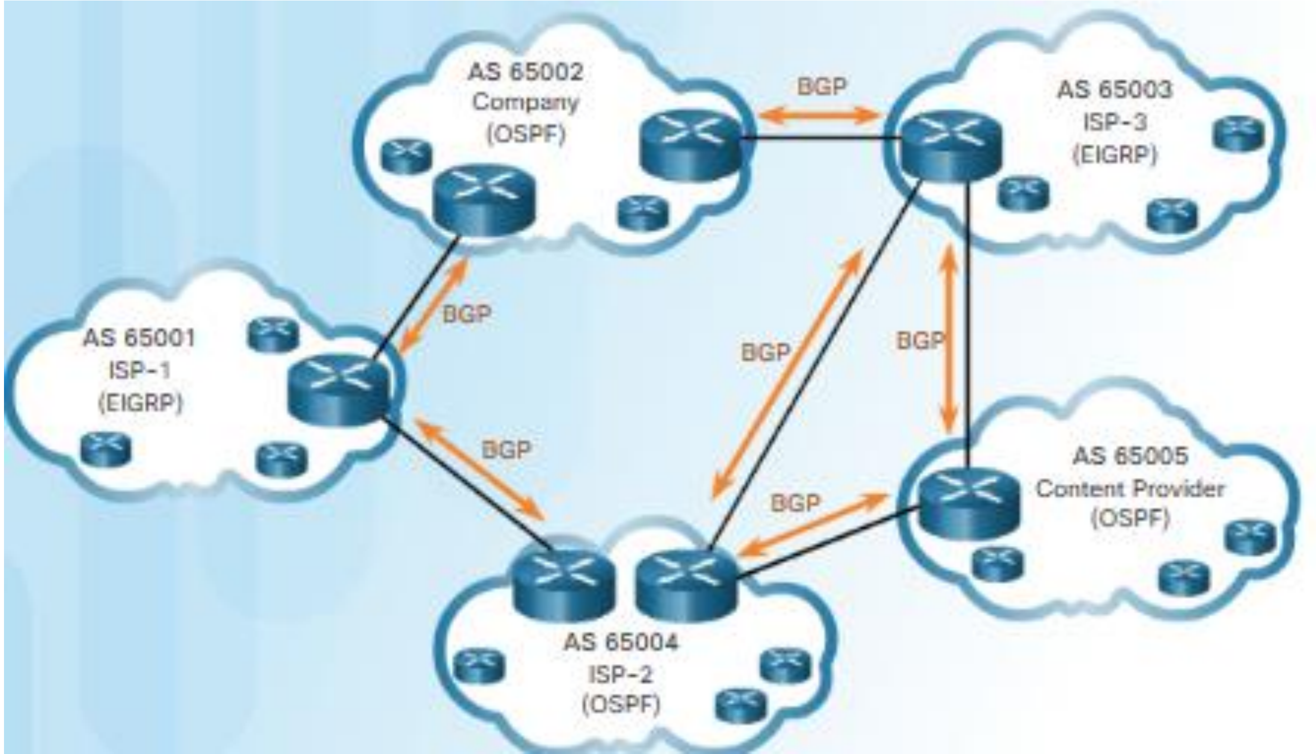

```
R1# show ip route


Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Dialer2
      10.0.0.0/32 is subnetted, 2 subnets
C        10.1.3.1 is directly connected, Dialer2
C        10.1.3.2 is directly connected, Dialer2
R1#
```




```
R1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A      1  30f7.0da3.1641  Gi0/1                   Di2 Vi2        UP
                30f7.0da3.0da1                              UP
R1#
```

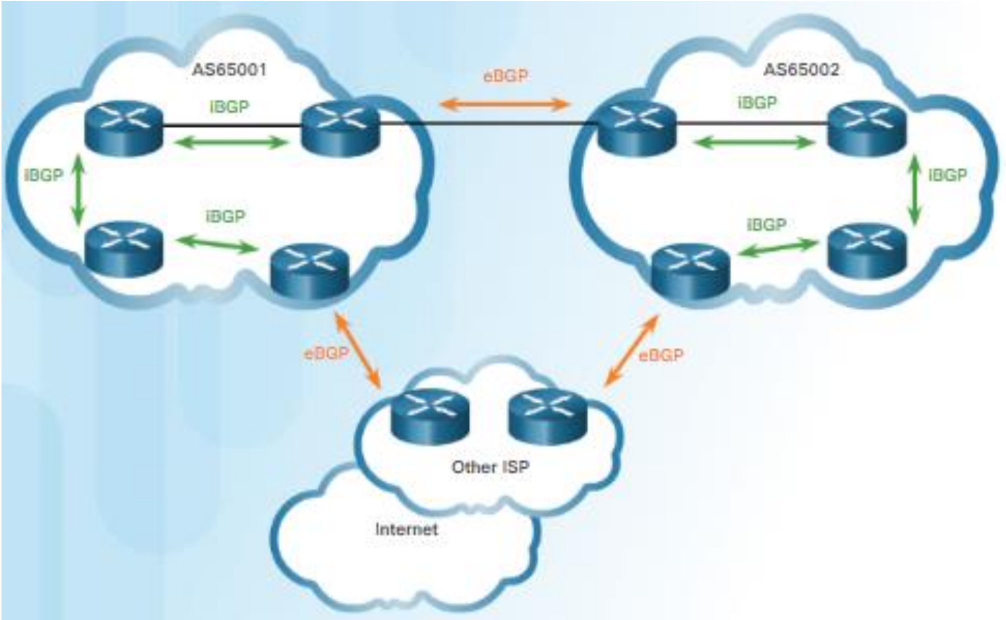
eBGP
BGP - Border Gateway Protocol

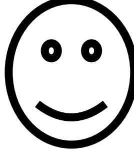
Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (**EGP**) used for the **exchange of routing information between autonomous systems**, such as ISPs, companies, and content providers (e.g., YouTube, Netflix, etc.).
In BGP, **every AS is assigned a unique 16-bit or 32-bit AS number** which uniquely identifies it on the Internet.
BGP updates are encapsulated over TCP on **port 179**. BGP inherits the **connection-oriented properties of TCP**, which ensures that BGP **updates are transmitted reliably**.



BGP - Border Gateway Protocol

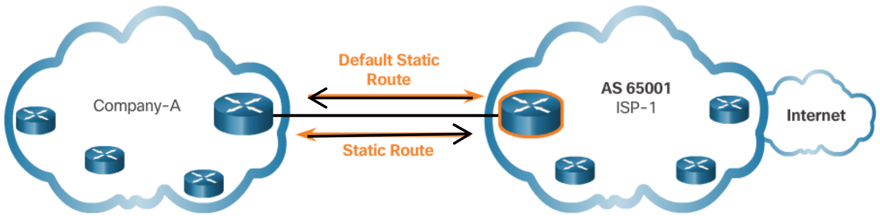
- IGP and EGP
  - Interior Gateway Protocols (**IGPs**) are used to exchange routing information **within a company network** or an autonomous system (AS).
  - Exterior Gateway Protocols (**EGPs**) are used for the exchange of routing information **between autonomous systems**.
- eBGP and iBGP
  - **External BGP** (**eBGP**) is the routing protocol used between routers in different autonomous systems.
  - Internal BGP (iBGP) is the routing protocol used between routers in the same AS.
- This course focuses on eBGP only.
- RFC 4271



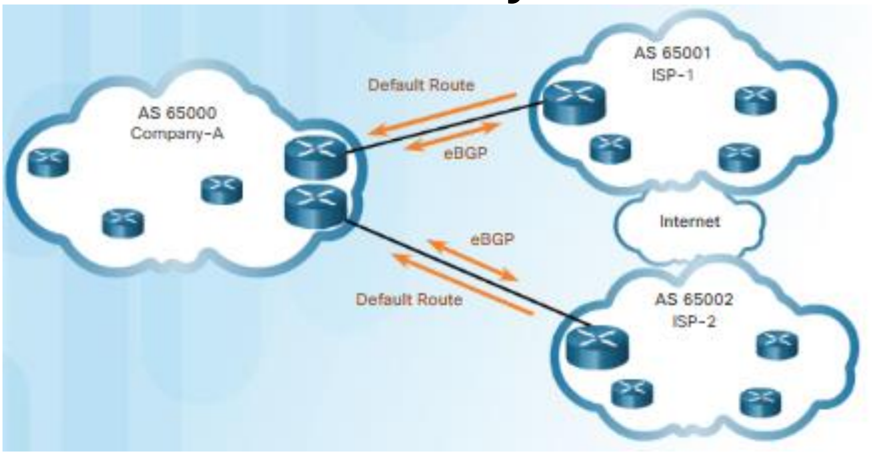


BGP Design Considerations

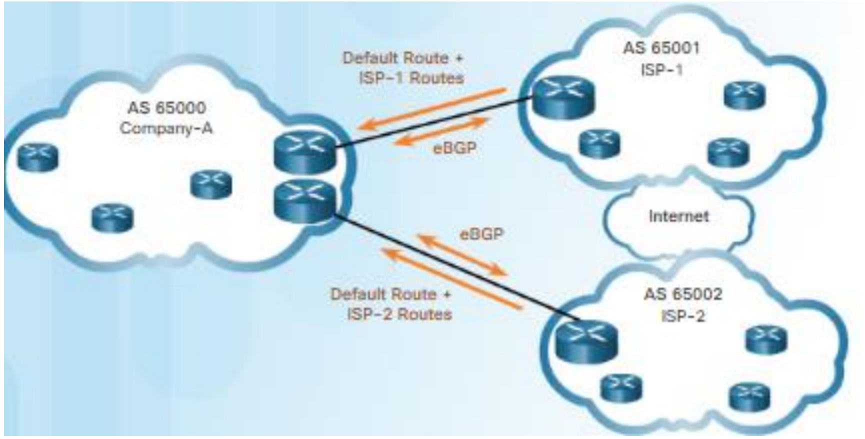
Single-Homed



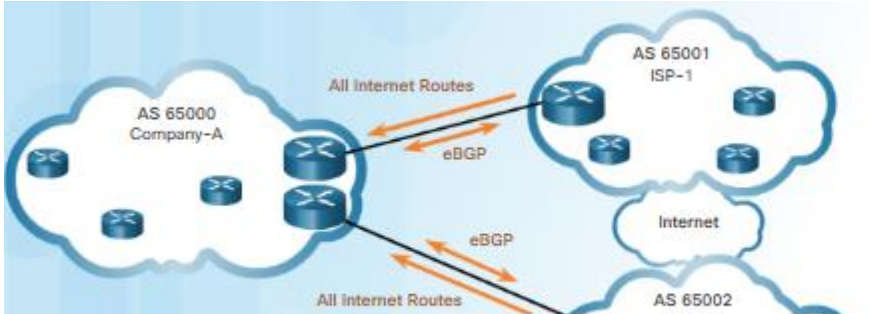
Default Route only



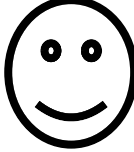
Default Route + ISP Routes



all Internet Routes



BGP Design Considerations



- BGP Options
  - There are three common ways an organization can choose to implement BGP in a **multi-homed** environment:
    - **Default Route Only** - This is the simplest method to implement BGP. However, because the company only receives **a default route from both ISPs**, sub-optimal routing may occur.
    - **Default Route and ISP Routes** - This option allows Company-A to **forward traffic to the appropriate ISP** for networks advertised by that ISP.
    - **All Internet Routes** - Because Company-A **receives all Internet routes from both ISPs**, Company-A can determine which ISP to use as the best path to forward traffic for any network. Although this solves the issue of sub-optimal routing, the **Company-A's BGP router must contain all Internet routes**.

      See: http://bgp.potaroo.net/

BGP Branch Configuration

- BGP Configuration Commands
  - There are three steps to implement BGP:
    - **Step 1**: Enable BGP routing.
    - **Step 2**: Configure BGP neighbor(s) (peering).
    - **Step 3**: Advertise network(s) originating from this AS.

Command	Description
Router(config)# **router bgp** *as-number*	Enables a BGP routing process, and places the router in router configuration mode.
Router(config-router)# **neighbor** *ip-address* **remote-as** *as-number*	Specifies a BGP neighbor. The as-number is the neighbor's AS number.
Router(config-router)# **network** *network-address* [**mask** *network-mask*]	Advertises a network address to an eBGP neighbor as being originated by this AS. The network-mask is the subnet mask of the network.

BGP Single-Homed Configuration

Company-A Configuration

```
Company-A(config)#router bgp 65000
Company-A(config-router)#neighbor 209.165.201.1 remote-as 65001
Company-A(config-router)#<>bnetwork 198.133.219.0 mask 255.255.255.0
```

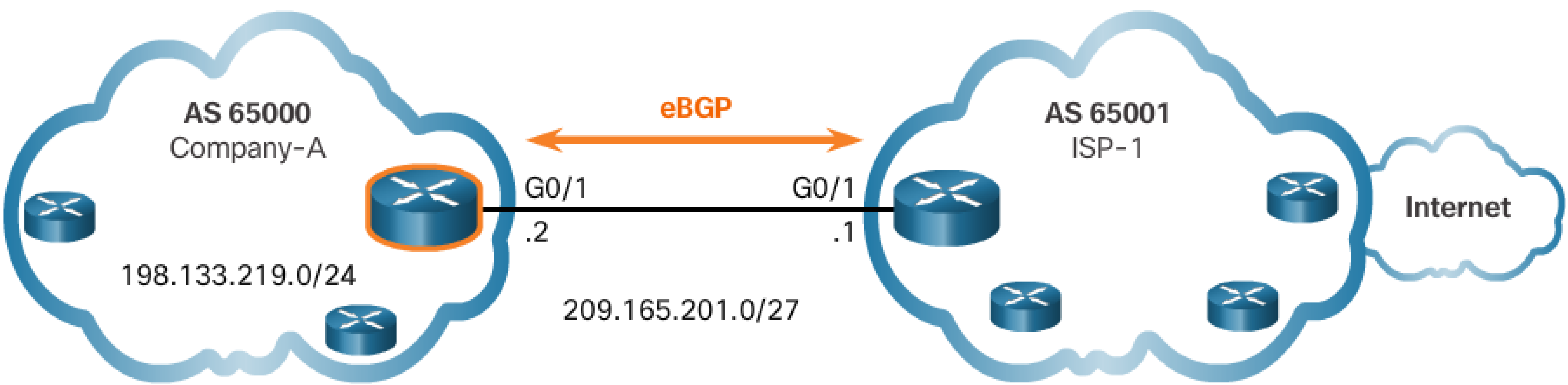
ISP-1 BGP Configuration

```
ISP-1(config)#router bgp 65001
ISP-1(config-router)#neighbor 209.165.201.2 remote-as 65000
ISP-1(config-router)#network 0.0.0.0
```

BGP Branch Configuration

- Verify eBGP
  - Three commands can be used to verify eBGP

Command	Description
Router# **show ip route**	Verify routes advertised by the BGP neighbor are present in the IPv4 routing table.
Router# **show ip bgp**	Verify that received and advertised IPv4 networks are in the BGP table.
Router# **show ip bgp summary**	Verify IPv4 BGP neighbors and other BGP information.



Summary

- **Broadband** transmission is provided by a wide range of technologies, including **DSL**, **fiber-to-the-home**, **coaxial cable systems**, **wireless**, and **satellite**. This transmission requires additional components at the home end and at the corporate end. Broadband wireless solutions include **municipal Wi-Fi**, **cellular/mobile**, and **satellite** Internet. Municipal Wi-Fi mesh networks are not widely deployed. Cellular/mobile coverage can be limited and bandwidth can be an issue. Satellite Internet is relatively expensive and limited, but it may be the only method to provide access.
- If multiple broadband connections are available to a particular location, a cost-benefit analysis should be performed to determine the best solution. The best solution may be to connect to **multiple service providers** to provide **redundancy and reliability**.
- **PPPoE** is a popular data link protocol for connecting remote networks to their ISPs. PPPoE provides the **flexibility of PPP** and the **convenience of Ethernet**.

Summary

- **VPNs** are used to create a **secure end-to-end private network connection over a third party network**, such as the **Internet**. **GRE** is a basic, **non-secure site-to-site VPN tunneling protocol** that can **encapsulate a wide variety of protocol packet types** inside IP tunnels, thus allowing an organization to **deliver other protocols through an IP-based WAN**. Today it is primarily used to **deliver IP multicast traffic or IPv6 traffic over an IPv4 unicast-only connection**.
- **BGP** is the routing protocol implemented **between autonomous systems**. Three basic design options for eBGP are as follows:
  - The ISP advertises **a default route only** to the customer
  - The ISP advertises **a default route and all of its routes** to the customer.
  - The ISP **advertises all Internet routes** to the customer.
- Implementing eBGP in a single-homed network only requires a few commands.