The bridge to possible

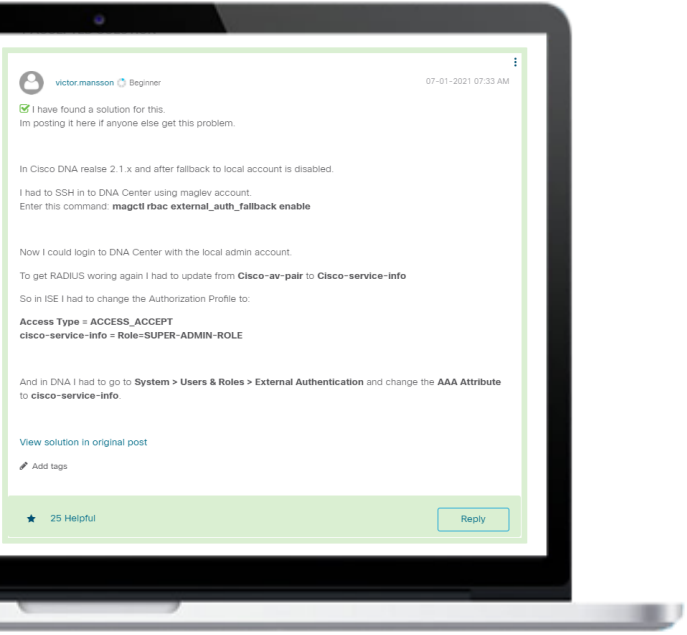
Sécurisez vos Protocoles de Routage RIP, EIGRP, OSPF, BGP et IS-IS

Community Live – Routage et Commutation

Alain Faure– CCIE #8935 R&S

19 Octobre 2021

Connect, Engage, Collaborate!



Lorsque vous recevez une réponse correcte, **acceptez-la comme solution !**

Cela aide les autres utilisateurs à trouver des réponses correctes

Mettez en évidence les autres membres

Les votes utiles motivent les membres enthousiastes en leur offrant **un signe de reconnaissance !**

© 2021 Cisco and/or its affiliates. All rights reserved.

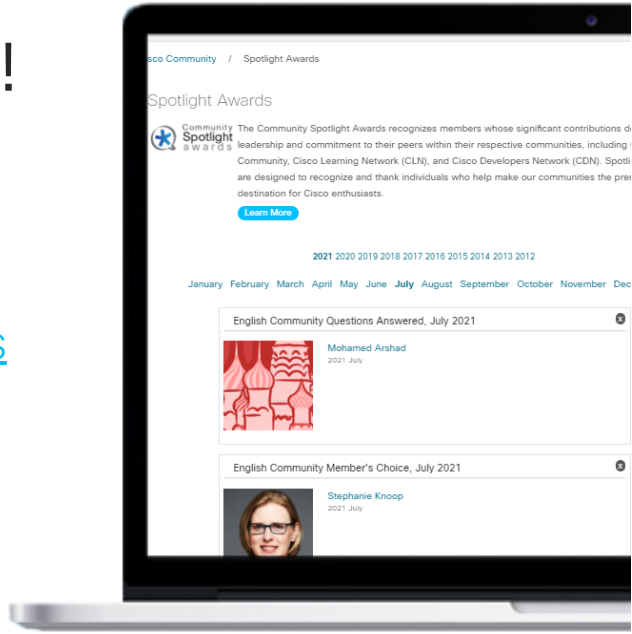
Spotlight Awards

De nouveaux lauréats chaque mois !

Gagnant du mois de Septembre : **Francois Vitet**

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les Spotlight Awards sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat ! Cliquez ici



© 2021 Cisco and/or its affiliates. All rights reserved.

Notre Expert

Alain Faure
Présentateur

Jimena Saez
Modérateur

[Téléchargez la présentation !]

© 2021 Cisco and/or its affiliates. All rights reserved.

Agenda

1. Introduction
2. RIP
3. OSPF
4. EIGRP
5. BGP
6. IS-IS

© 2021 Cisco and/or its affiliates. All rights reserved.

1. Introduction

Avant-propos

Vos souhaits

Rapidement, j'aimerai compléter la dernière présentation sur les certifications par 2 livres qui me semblent indispensables à lire, comprendre et relire (vérifiez que ce soit bien les dernières éditions) :

- Interconnections: bridges, routers, switches and internetworking protocols / Radia Perlman (2éme édition) (peut être existe t-il une version Française)- > Fondamental pour comprendre l'évolution des réseaux, aborde le sujet des graphes dans les réseaux
- Réseaux locaux et Internet. Des protocoles à l'interconnexion / Laurent Toutain (Paru en mars 2003) - > Précieux pour le comportement de TCP, d'UDP et de IP.

© 2021 Cisco and/or its affiliates. All rights reserved.

Présentation (1)

Rappel : Cisco est une entreprise fondée en 1984.

+75.000 personnes.

+de 35 ans d'expérience dans le développement des routeurs

Cisco contribue fortement à l'équipement de l'infrastructure d'Internet grâce à ses routeurs.

© 2021 Cisco and/or its affiliates. All rights reserved.

Présentation (2)

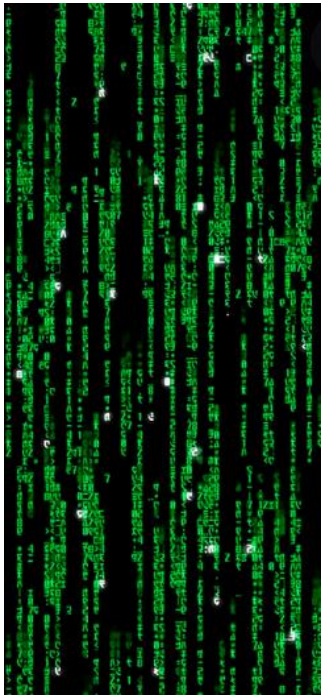
Cette présentation s'adresse à des spécialistes réseaux, pour leur permettre de faire un point pratique sur l'aspect sécurisation des protocoles réseaux (RIP, EIGRP, OSPF, BGP et IS-IS ; IPv4/IPv6).

Bien sûr, il est nécessaire de se tenir au courant des éventuelles failles découvertes et corrigées, mais je veux parler des solutions mises en place à l'installation ou configurées de manière planifiée.

© 2021 Cisco and/or its affiliates. All rights reserved.

Meilleures pratiques et Points d'attention

- Attention aux routes redistribuées (en provenance d'un autre domaine de routage)
- Rien n'est prévu de base pour sécuriser à 100 %. Internet a été mis en place dans les années 80-90 entre gens de «bonne compagnie».
- Si vous ne pouvez/souhaitez pas mettre en place la sécurisation du protocole, sécurisez l'infra sous-jacente. Vous pouvez imaginer un système de script pour valider l'installation d'un routeur légitime dans votre réseau et rejeter les autres. Mais alors cela ressemble beaucoup aux solutions SDN du type SD-WAN.



© 2021 Cisco and/or its affiliates. All rights reserved.

SDN

Il faut garder à l'esprit qu'il existe aussi des solutions comme SD-WAN qui augmentent bien entendu la sécurité de l'infrastructure réseau grâce à leur mécanisme d'authentification intrinsèque.

Voir la présentation SD-WAN de la communauté francophone Cisco :

- SD-WAN: Routage et Commutation / Documents de Routage et Commutation « SD-WAN : Viptela OS avec vEdge et vManage»

© 2021 Cisco and/or its affiliates. All rights reserved.

Polling Question 1

Quel est le mode le plus sécurisé de RIPv3 ?

1) aucun
2) Mot de passe en clair
3) Hash md5
4) Ipsec

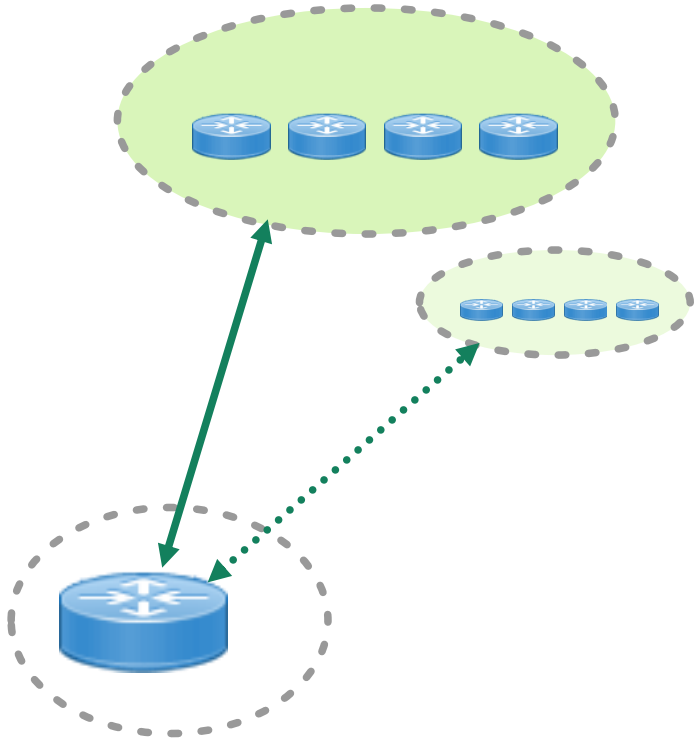
© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2. RIP

RIPv2

RIP peut paraître comme un protocole dépassé, mais il peut être utilisé entre un site central et des petites succursales locales.

(EIGRP peut aussi être utilisé dans ce but)



© 2021 Cisco and/or its affiliates. All rights reserved.

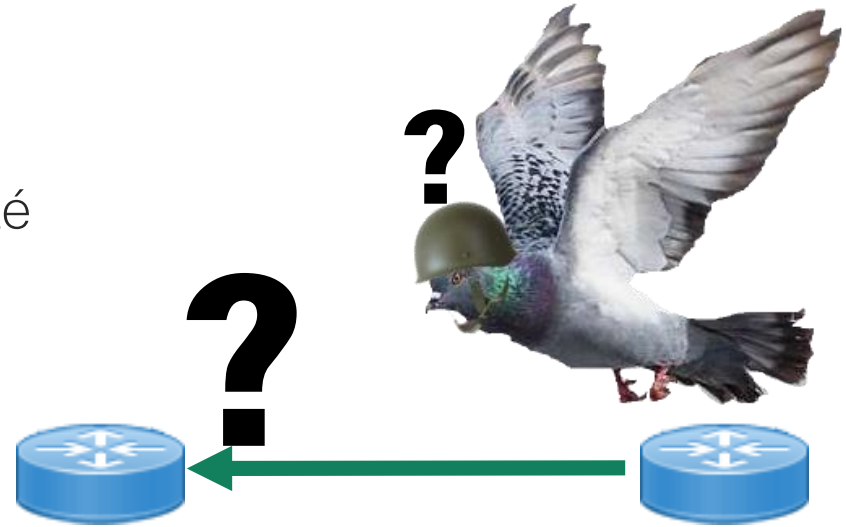
RIPv2

RFC 2453

Protocole : UDP 520

Mode non sécurisé :

- Pas d'authentification de la source
- Pas d'assurance sur la confidentialité des routes
- Attention équipements de fin de chaîne = plus ou moins bien protégés

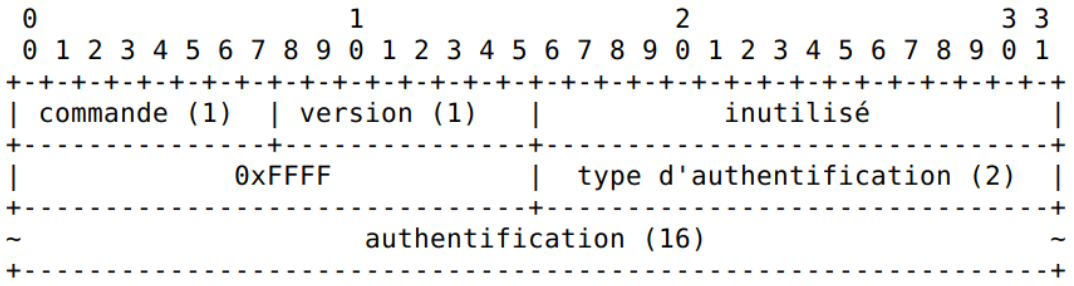


© 2021 Cisco and/or its affiliates. All rights reserved.

RIPv2 : Solutions

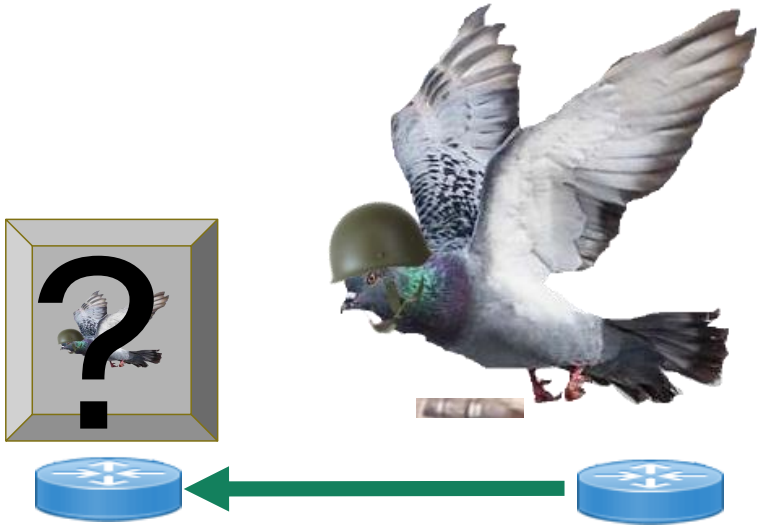
RFC 2453

- RFC : authentif. en clair
- Cisco : authentif. MD5



Référence :

- https://www.cisco.com/c/fr_ca/support/docs/ip/routing-information-protocol-rip/13719-50.html



© 2021 Cisco and/or its affiliates. All rights reserved.

RIPv2 : Configuration authent. en clair

```
key chain pigeon
key 1
key-string ramier
```

```
interface FastEthernet 0
ip address 172.16.1.1 255.255.0.0
ip rip authentication key-chain pigeon
```

```
router rip
version 2
network 172.16.0.0
```

```
key chain pigeon
key 1
key-string ramier
```

```
interface FastEthernet 0
ip address 172.16.2.2 255.255.0.0
ip rip authentication key-chain pigeon
```

```
router rip
version 2
network 172.16.0.0
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Rappel : hash MD5

Principe du hash (aussi SHA1):

1000 -> 1 xor 0 ; 0 xor 0 = 10

1010 -> 1 xor 0 ; 1 xor 0 = 11

0100 -> 0 xor 1 ; 0 xor 0 = 10

Conséquence 10 != 11

Impossible de retrouver L'origine :

10 -> ? 1000 ? 1010 ? 0100

Voir: https://fr.wikipedia.org/wiki/MD5

Analystes : N'oubliez pas de saler les mots de passe !

© 2021 Cisco and/or its affiliates. All rights reserved.

RIPv2 : Configuration authent. md5

```
key chain pigeon
key 1
Key-string ramier
```

```
interface FastEthernet 0
ip address 172.16.1.1 255.255.0.0
ip rip authentication mode md5
ip rip authentication key-chain pigeon
```

```
router rip
version 2
network 172.16.0.0
```

```
key chain pigeon
key 1
Key-string ramier
```

```
interface FastEthernet 0
ip address 172.16.2.2 255.255.0.0
ip rip authentication mode md5
ip rip authentication key-chain pigeon
```

```
router rip
version 2
network 172.16.0.0
```

© 2021 Cisco and/or its affiliates. All rights reserved.

RIPv2 : Debug

Authentification texte :

```
debug ip rip

RIP: received packet with text authentication ramier
```

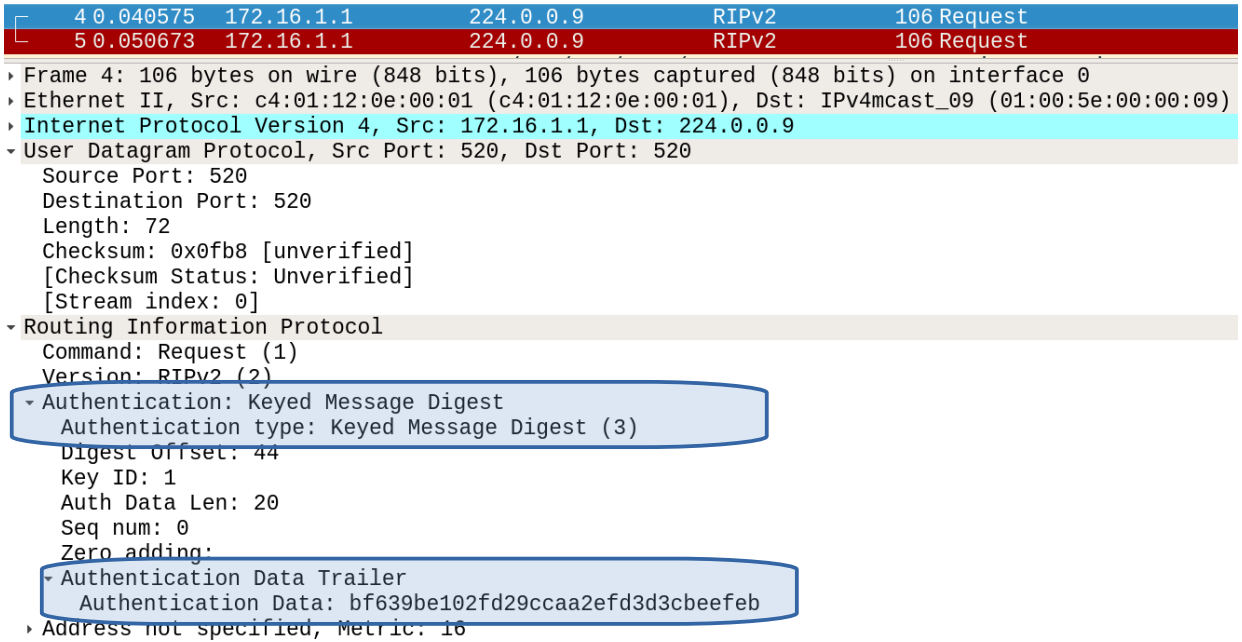
Authentification md5 :

```
debug ip rip

RIP: received packet with md5 authentication
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Capture wireshark

Avec MD5 :



© 2021 Cisco and/or its affiliates. All rights reserved.

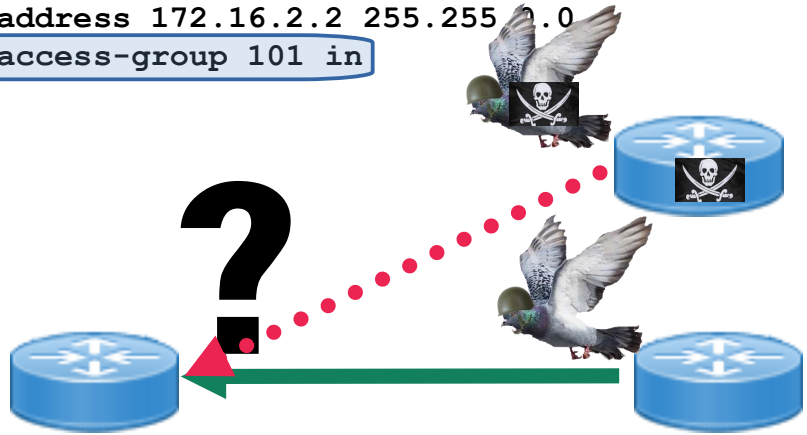
Autres mécanismes - access-list

Empêcher un routeur pirate :

Quand la sécurité est vraiment un problème, il est bon aussi de compléter le dispositif par des access-lists.

```
access-list 101 permit udp host 172.16.2.1
eq 520 any eq 520
access-list 101 deny udp any eq 520 any eq
520
access-list 101 permit ip any any
```

```
interface FastEthernet 0
ip address 172.16.2.2 255.255.0.0
ip access-group 101 in
```

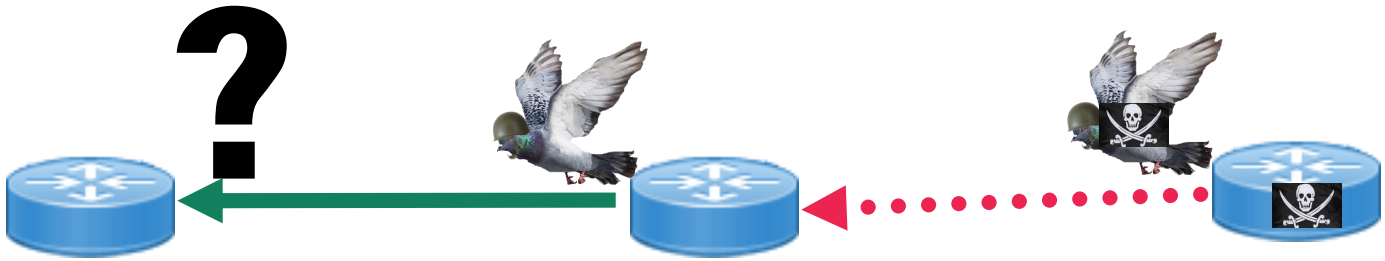


© 2021 Cisco and/or its affiliates. All rights reserved.

Autres mécanismes - distribute-list

Listes de distribution : Contrôle de la circulation des routes à l'entrée et à la sortie du routeur.

```
router rip
version 2
network 10.0.0.0
network 172.16.0.0
distribute-list SOUSRESEAU in
no auto-summary
!
ip access-list standard SOUSRESEAU
permit 1.1.1.0 0.0.0.255
```



© 2021 Cisco and/or its affiliates. All rights reserved.

Autres mécanismes - passive-interface

Interface Passive :

Elle évite d'envoyer sur certaines interfaces les paquets multicast du protocole RIP.

Mais ne l'empêche pas de recevoir ces paquets.

Note : Je ne reviendrais pas sur ces 4 derniers mécanismes, mais ils sont applicables pour d'autres protocoles

```
router rip
version 2
network 10.1.1.0
passive-interface ethernet 0/0
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Vérification

Vérifiez les numéros de réseaux qui arrivent dans la table de routage sont bien légitimes.

Un process que vous pouvez automatiser avec un logiciel de supervision de réseau :

```
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M -
mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o -
ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.0.0/16 is directly connected, GigabitEthernet0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Et IPv6 ?

RIP IPv6 s'appelle RIPng il est actif sur le port UDP 512.

Multicast : ff02::9

La philosophie de IPv6 est un peu différente : C'est la couche Ipsec (donc hors RIPng) qui est chargée du chiffrage des communications et donc de la protection pour l'authentification et le chiffrage (cryptage) des données de routage.

Je vais montrer un exemple de configuration d'IpSec pour RIPng, mais le principe reste le même pour EIGRP IPv6 ou OSPFv3 :

On s'appuie sur un tunnel Ipsec de manière tout à fait indépendante du protocole de routage.

Idem pour EIGRP IPv6 et OSPFv3 il faut désactiver ces protocoles sur l'interface matérielle

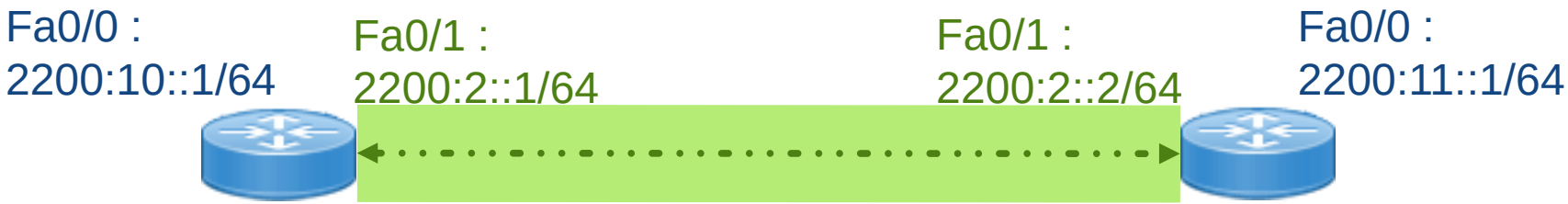
© 2021 Cisco and/or its affiliates. All rights reserved.

RIPng et tunnel Ipsec (1)

Nous allons revoir la base de la configuration :

On déclare le protocole de routage, les réseaux et le tunnel.

```
ipv6 unicast-routing
!
interface fastEthernet 0/0
ipv6 address 2200:10::1/64
ipv6 rip pigeon enable
ipv6 enable
no shut
!
interface fastEthernet 0/1
ipv6 address 2200:2::1/64
ipv6 enable
no shut
```



© 2021 Cisco and/or its affiliates. All rights reserved.

RIPng et tunnel Ipsec (2)

Configuration du tunnel.

```
interface tunnel01
ipv6 address 2200:3::1 link-local
ipv6 address 2200:3::1/64
ipv6 rip pigeon enable
ipv6 enable
tunnel source FastEthernet0/1
tunnel destination 2200:2::2
tunnel mode ipsec ipv6
tunnel protection ipsec profile profile0
no shut
```

© 2021 Cisco and/or its affiliates. All rights reserved.

RIPng et tunnel Ipsec (3)

ISAKMP : Internet Security Association and Key management Protocol.

ASSOCIATION de SECURITE (SA)

La clé (mot de passe partagé) :

cisco

Phase I

```
crypto isakmp key cisco address ipv6
2200:2::1/128
!
crypto isakmp policy 10
   encr 3des
   hash md5
   authentication pre-share
   Lifetime 3600
!
!
!
crypto ipsec transform-set 3des ah-sha-hmac
esp-3des
!
crypto ipsec profile profile0
   set transform-set 3des
```

© 2021 Cisco and/or its affiliates. All rights reserved.

RIPng et tunnel Ipsec (4)

Configuration du profile Ipsec du tunnel.

Caractéristiques «négociées»

AH : Authentification Header

ESP : Encapsulating Security Payload

```
crypto isakmp key cisco address ipv6
2200:2::1/128
!
crypto isakmp policy 10
   encr 3des
   hash md5
   authentication pre-share
   Lifetime 3600
!
!
!
!
!
!
crypto ipsec transform-set 3des ah-sha-hmac
esp-3des
!
crypto ipsec profile profile0
   set transform-set 3des
```

Phase II

© 2021 Cisco and/or its affiliates. All rights reserved.

Polling Question 2

Quel est la définition de NSSA ?

1) National Security & Secret Agency
2) No Secure System Admin
3) Not So Stubby Area
4) National Secret System Authentication

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3. OSPF

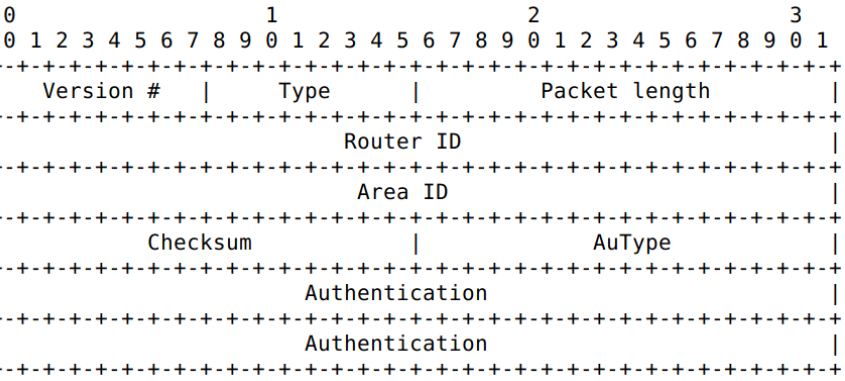
OSPF

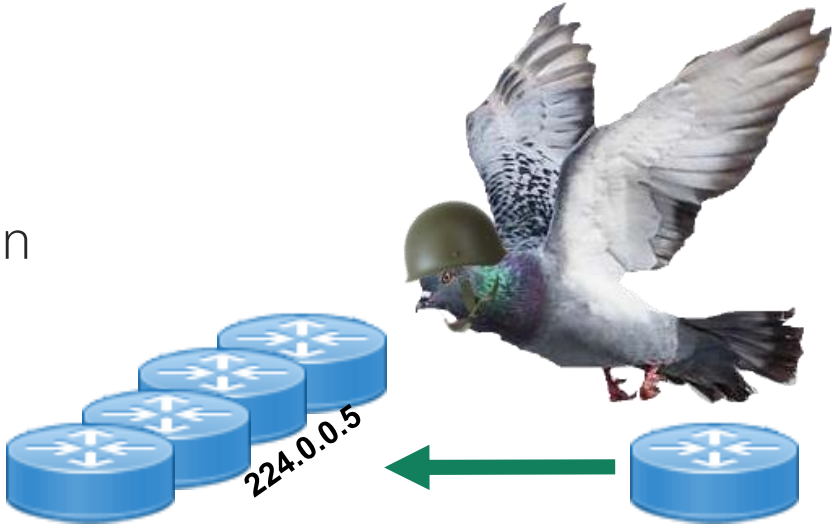
OSPFv2 : RFC 2328

Protocole : Multicast pour envoyer de l'info à tous les routeurs : 224.0.0.5

Et vers les DR/BDR : 224.0.0.6

Mais dans le cas des réseaux non-broadcast (liens WANs), il faut mettre en place des liaisons unicast.





© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2: Classique

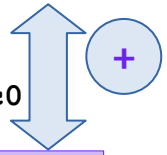
Comme RIPv2 il y a un mécanisme d'authentification on en trouve 2 types (clair, md5) et cela peut se faire par :

- Lien
- Area

Comme avec RIPv2 il est possible de filtrer les routes pour s'assurer qu'elles sont valides.

Pour l'interface

```
interface FastEthernet 0
ip address 192.16.64.2 255.255.255.0
ip ospf message-digest-key 1 md5 c1$c0
```



Pour toute l'area

```
router ospf 10
network 70.0.0.0 0.255.255.255 area 0
area 0 authentication message-digest
```

```
show ip ospf interface FastEthernet 0
...
Message digest authentication enabled
Youngest key id is 1
```

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2:avec HMAC-SHA

A partir de la version 15.4T on dispose d'une signature HMAC-SHA (Hash Message Authentication Code Secure Hash Algorithm ; RFC 5709)

Vous devez veiller aussi à ce que les clés de différents réseaux soit différentes .

```
key chain R1
key 1
cryptographic-algorithm hmac-sha-512
key-string mot_de_passe
```

Pour l'interface

```
interface FastEthernet 0
ip address 192.16.64.2 255.255.255.0
ip ospf authentication
ip ospf authentication key-chain R1


router ospf 10
network 70.0.0.0 0.255.255.255 area 0
```

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2: Autres Solutions

Vous pouvez mettre en place d'autres mesures de sécurisation :

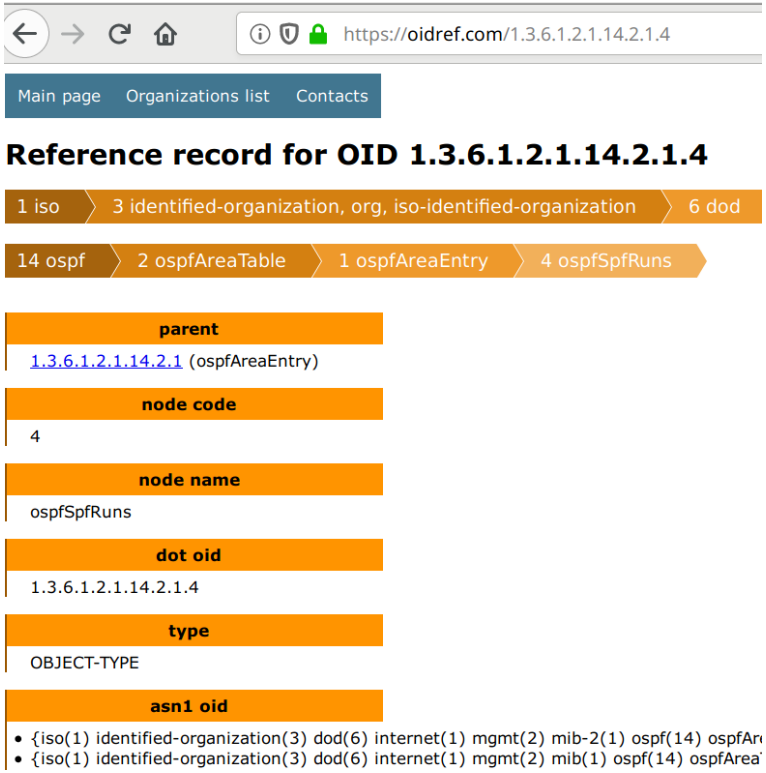
- Utilisation de «**`passive`**» sur les interfaces
- Vérification par «RPF Reverse Path Forwarding»
- Vérification des adresses IP aux frontières du domaine
- Vérification du TTL (Time To Live)

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2:Surveillez le nb de process OSPF

Gardez un œil sur le nombre de process OSPF par : OspfSpfRuns dans la MIB OSPF (snmp)

Vous pouvez prévoir des scripts qui vont vérifier la cohérence de la base de donnée OPSF. En particulier surveillez qu'il n'y ai pas d'ASBR en trop.

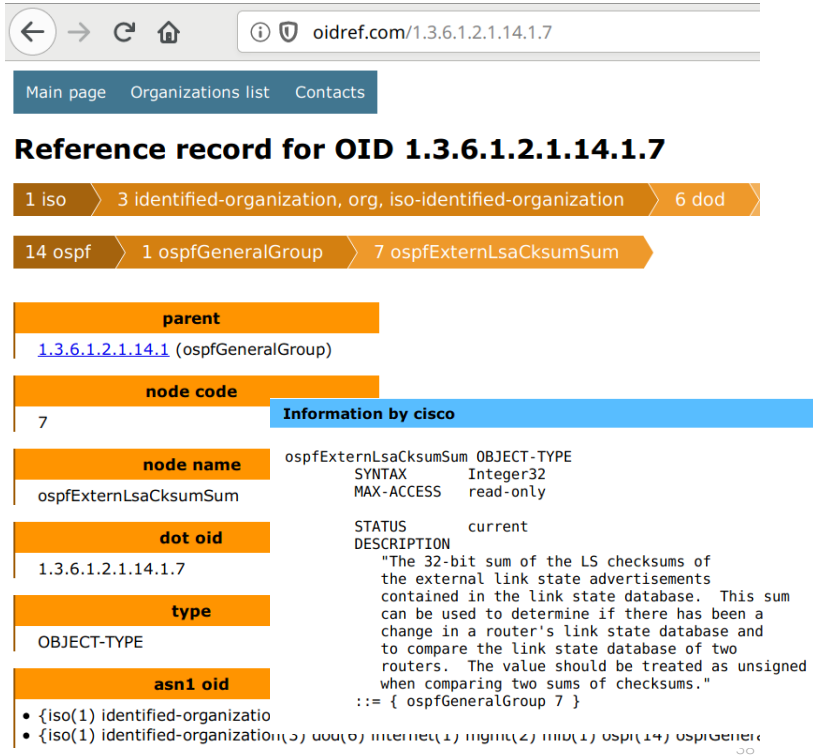


© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2:Vérifiez la cohérence des check-sum

Ayez un process qui surveille la cohérence des check-sum. Par exemple pour ospfExternLsaCksumSum dans la MIB OSPF (snmp)

Vous pouvez prévoir des scripts qui vont vérifier la cohérence des check-sum des LSAs.



© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2:Limitez le TTL

Autorisez la sécurisation par TTL. Voir : https://www.cisco.com/c/en/us/td/docs/ios/iproute_ospf/configuration/guide/iro_ttl.html?dtid=osscdc000283

Exemple TTL + «shutdown gracieux» :

```
R1 :
interface ethernet 0/1
ip ospf ttl-security hops 5

R2 :
interface ethernet 0/1
ip ospf ttl-security

R1 :
router ospf 1
ttl-security all-interfaces
```

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2:Cachez ces réseaux que je ne saurais voir

Possibilité de cacher des réseaux réservés au transit (selon RFC 6860).

Voir : https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/213404-open-shortest-path-first-prefix-suppress.html

Exemple de suppression des préfix :

```
R1 :
router ospf 1
prefix-suppression
interface ethernet 0/1
ip ospf prefix-suppression

R2 :
router ospf 1
prefix-suppression
interface ethernet 0/1
ip ospf prefix-suppression
```

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2:Utilisez les U-interfaces

Le comportement des «unnumbered interfaces» est intéressant :

- pas de host route

- pas de paquets vers l'interface (adresse)

Exemple de unnumbered interface :

```
R1 :
interface ethernet 0/10
ip unnumbered ethernet 0/0
```

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv2:Vérifez le RPF

RPF : Reverse Path Forwarding

Exemple de Configuration RPF :

```
R1 :
interface ethernet 0/10
ip verify unicast reverse-path
```

Je vérifie si l'@ de R est bien dans la direction que je connais pour R

R annonce qu'il sait où se trouve 192.168.1.0/24

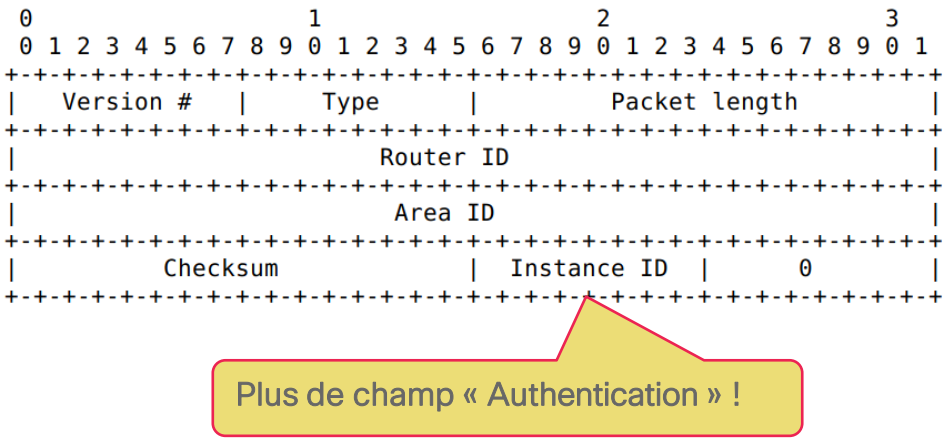
© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv3 :

Avec OSPFv3 (RFC2740), l'entête d'authentification n'est plus là. On utilise un tunnel Ipsec.

Voir : IPv6 Routing: OSPFv3 Authentication Support with Ipsec (Configuration Guide Cisco)

RFC4552: Authentification/confidentialité pour OSPFv3 in french : http://abcdrfc.free.fr/rfc-vf/pdf/rfc4552.pdf



© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv3 : Authentification (1)

Avec OSPFv3

Voir : IPv6 Routing: OSPFv3 Authentication Support with Ipsec (Configuration Guide Cisco)

```
R1
interface FastEthernet 0
ipv6 ospf area 1
ipv6 ospf authentication spi 256 sha1 -signature sha1-

R2
interface FastEthernet 0
ipv6 ospf area 1
ipv6 ospf authentication spi 256 sha1 -signature sha1-
```

Pour toute l'interface

```
ou
interface FastEthernet 0
ipv6 ospf area 1
ospfv3 authentication md5 0
761340947681324733020312097 27
```

Au choix

```
area 0 authentication ipsec spi 256  sha1 -signature
sha1-
```

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv3 : Authentification (2)

Avec OSPFv3, on utilise un tunnel Ipsec.

```
R1
ipv6 router ospf 1
router-id 10.11.11.1
area 0 authentication ipsec spi 1000 md5 4567890ABCDEF1234567890
```

Voir : IPv6 Routing: OSPFv3 Authentication Support with Ipsec (Configuration Guide Cisco)

© 2021 Cisco and/or its affiliates. All rights reserved.

OSPFv3 : Authentification Attachée (Trailer)

À lire : RFC 6506

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-12/configuration_guide/rtng/b_1612_rtng_9300_cg/configuring_ospfv3_authentication_trailer.html

```
key chain ospf-1
key 1
key-string ospf
cryptographic-algorithm hmac-sha-256

interface GigabitEthernet 1/0/1
ospfv3 1 ipv6 authentication key-chain ospf-1

router ospfv3 1
address-family ipv6 unicast
area 1 authentication key-chain ospf-1
area 1 virtual-link 1.1.1.1 authentication key-chain ospf-1
area 1 sham-link 1.1.1.1 authentication key-chain ospf-1
authentication mode deployment
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Polling Question 3

Quel est la définition de DUAL ?

1) Double Unit Area Line
2) Double Unit Area Link
3) Diffusing Update Algorithm
4) Double Update for All Link

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4. EIGRP

EIGRP : Un protocole Cisco

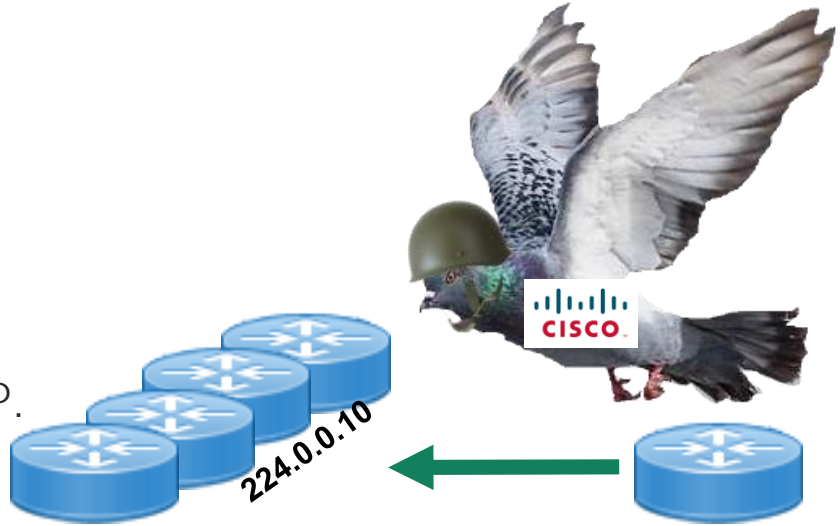
EIGRP : RFC 7868

Protocole : Multicast pour envoyer de l'info à tous les routeurs :

224.0.0.10 IPv4 et ff02::a IPv6

Un excellent document d'introduction sur EIGRP : DGTL-BRKENT-1102 EIGRP Introduction and Overview Steven Moore CCIE #4927 à LIVE CISCO 2020

Il y a les mécanismes que j'ai traité pour RIP. Donc je ne vais pas les représenter ici. Simplement vous donner les références :



© 2021 Cisco and/or its affiliates. All rights reserved.

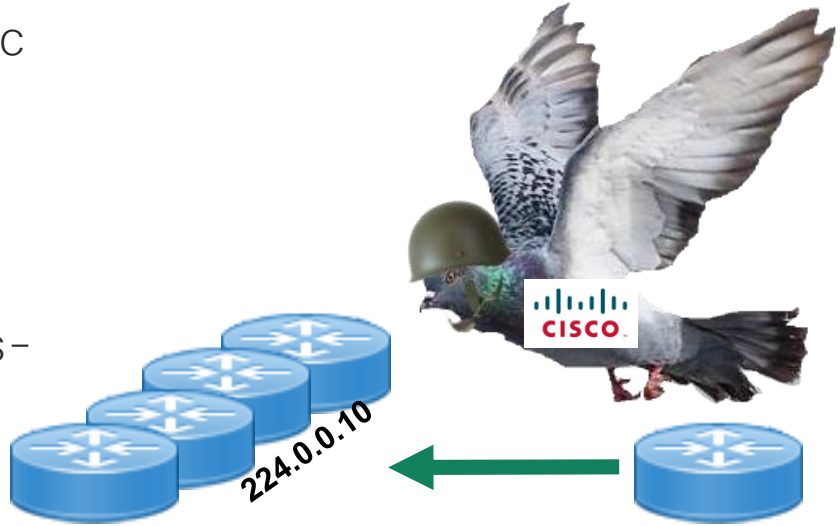
EIGRP : Un protocole Cisco

Document Cisco sur la sécurisation des échanges EIGRP (cela ressemble beaucoup à RIP):

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/82110-eigrp-authentication.html

Et

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16/ire-xe-16-book/ire-sha-256.html



© 2021 Cisco and/or its affiliates. All rights reserved.

EIGRP : Configuration authent. md5

```
key chain pigeon
key 1
Key-string ramier

interface FastEthernet 0
ip address 172.16.1.1 255.255.0.0
ip authentication mode eigrp 57 md5
ip authentication key-chain eigrp 57
pigeon

router eigrp 57
network 172.16.0.0
```

```
key chain pigeon
key 1
Key-string ramier

interface FastEthernet 0
ip address 172.16.2.2 255.255.0.0
ip authentication mode eigrp 57 md5
ip authentication key-chain eigrp 57
pigeon

router eigrp 57
network 172.16.0.0
```

Syntaxe diff. de RIP

© 2021 Cisco and/or its affiliates. All rights reserved.

EIGRP : Passive interface

La commande «passive interface» sur eigrp supprime toute adjacence, cela fait que les routes ne sont ni émises, ni surtout reçues.

```
router eigrp 89
passive-interface FastEthernet 0
```

Différent de RIP

Pour avoir le même comportement qu'en RIP utilisez une «distribute-list».

© 2021 Cisco and/or its affiliates. All rights reserved.

Polling Question 4

Est-ce que le n° d'AS 65536 est privé ?

1) Oui
2) Non

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

5. BGP

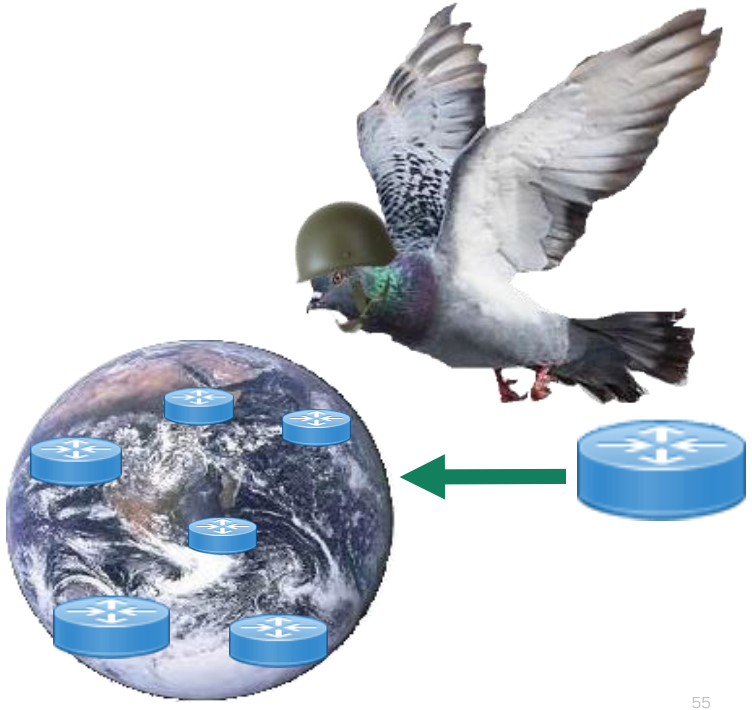
BGP : Le protocole d'Internet

BGP 4 : RFC 4271

Multiprotocol BGP : RFC 4760

Un bon article à lire :
https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_du_Border_Gateway_Protocol

Notez que BGP sert pour tout un tas d'applications -Ex : liens secours à travers des firewalls (iBGP)-



© 2021 Cisco and/or its affiliates. All rights reserved.

BGP : Le protocole d'Internet

Avec BGP, quelques exemple de risques:

- Manipulation de la table de routage

BGP spoofing (lire : « BGP spoofing – why nothing on the internet is actually secure » – 2013 – recherche google)

- BGP DDOS

© 2021 Cisco and/or its affiliates. All rights reserved.

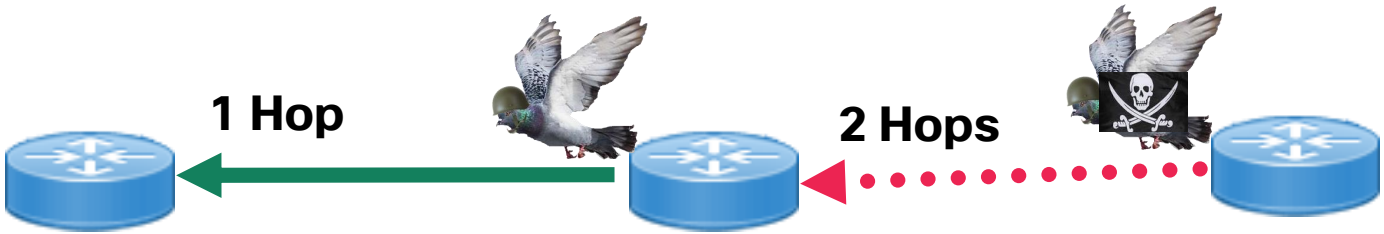
BGP : Vérification du TTL

La première technique possible est la vérification du TTL (Time To Live). Il s'agit en fait de déterminer en avance le nombre de hop maximum entre deux voisins.

Doit être configuré des deux cotés.

TTL max. = 255 - Nb de hops

```
router bgp 10
neighbor 10.0.0.20 remote-as 20
neighbor 10.0.0.20 ttl-security hops 1
```



© 2021 Cisco and/or its affiliates. All rights reserved.

BGP : Authentification par mot de passe

Le mot de passe permet l'identification. En fait c'est un hash MD5 qui est envoyé de l'autre coté.

```
router bgp 10
neighbor 10.0.0.20 remote-as 20
neighbor 10.0.0.20 password mot2passe
```

Les deux coté doivent être configurés de manière identique.

© 2021 Cisco and/or its affiliates. All rights reserved.

BGP : Logger les événements

Permet de récupérer les logs, intéressant pour les faire examiner en temps réel.

Montre l'activité des routeurs connectés.

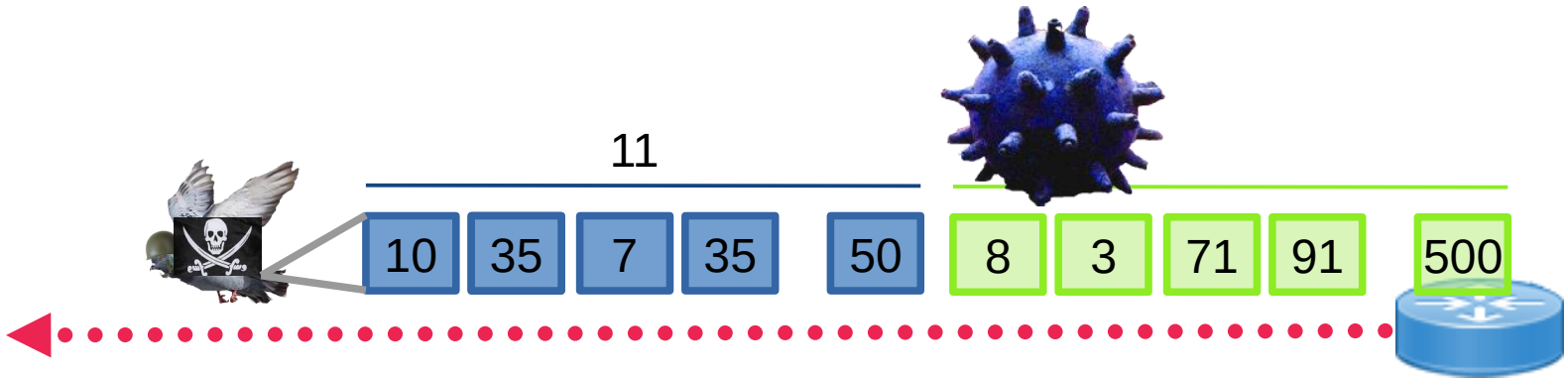
```
router bgp 10
bgp log-neighbor-changes
```

© 2021 Cisco and/or its affiliates. All rights reserved.

BGP : Limitez le nombre d'AS empilés

Permet d'éviter que le chemin vers un préfixe dépasse un nb d'AS évidement trop important.

```
router bgp 10
bgp maxas-limit 11
```



© 2021 Cisco and/or its affiliates. All rights reserved.

BGP : Evitez d'importer/d'exporter certains prefix

Filter le plus possible les prefix en entrée et en sortie.

Utilisez le maximum prefix pour signaler quand la table se rempli trop.

```
router bgp 10
neighbor 10.0.0.20 prefix-list NON in
neighbor 10.0.0.20 prefix-list OUI out
neighbor 10.0.0.20 maximum-prefix 100
```

```
ip prefix-list OUI seq 2 permit 20.2.2.0/24
ip prefix-list OUI seq 6 deny 0.0.0.0/0 le 32

ip prefix-list NON seq 2 permit 10.1.1.0/24
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Références à lire

Il y a beaucoup de littérature sur le sujet de la sécurité du protocole BGP, qlq exemples en Français:

- Bonnes pratiques de configuration de BGP / ANSSI sept. 2013
- « Quelques éléments de sécurité autour du protocole de routage BGP » google (2008)
- Un MUST : BRKSPG-3012 SP Security Leveraging BGP FlowSpec to protect your infrastructure - Nicolas Fevrier – 2018 Live Cisco Barcelone

- Article Cisco Press (in english) : https://www.ciscopress.com/articles/article.asp?p=1237179

© 2021 Cisco and/or its affiliates. All rights reserved.

BGP Flowspec (lire RFC 5575)

C'est une fonctionnalité qui a été très bien couverte et en détail dans une présentation au LIVE Cisco. Vous pouvez la trouver sur le site de Cisco LIVE de 2018 à Barcelone.

BRKSPG-3012

SP Security : **Leveraging BGP FlowSpec to protect your infrastructure**

Nicolas Fevrier, Technical Leader Engineering

@CiscoIOSXR

© 2021 Cisco and/or its affiliates. All rights reserved.

Agenda

- Introduction
- BGP FlowSpec Protocol Description
- Use-cases, Demo w/ DDoS Mitigation
- Configuring the Protocol
- Caveats and Limitations
- Conclusion

Cisco live!

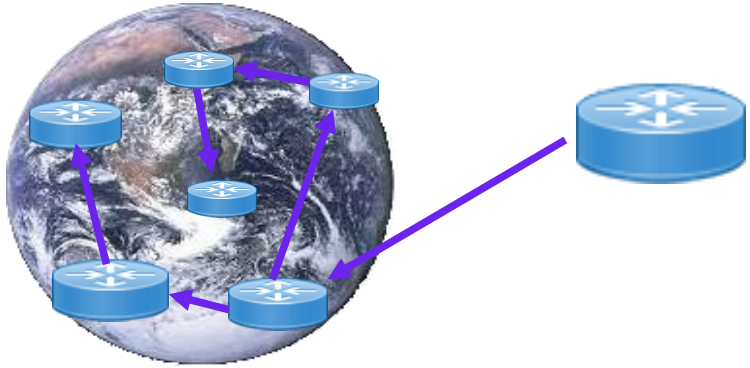
BGP Flowspec – intro

RFC 8955 : « Dissemination of Flow Specification Rules »

RFC8956 pour IPv6

Le principe est qu'un contrôleur central est utilisé pour diffuser une politique (les règles) de traitement des informations arrivant par les interfaces des routeurs clients.

Une des utilisation est la sécurité avec la possibilité de faire échec à une attaque DDOS.



© 2021 Cisco and/or its affiliates. All rights reserved.

BGP Flowspec – Règles

A droite on peut voir un exemple de règle :

- Condition de trafic
- Action si condition de trafic rencontrée

Traffic Description	Action
dst:2001:4:5::23/128	redirect-in-VRF Dirty
UDP:123 Size: 800-1500	rate-limit 0 bps
dst:1.2.3.4 SYN	redirect-to-IP 20.2.3.4
src:4.0.0.1 TCP80	mark DSCP ef

On comprends que ce type de règles peut servir à divers objectifs.

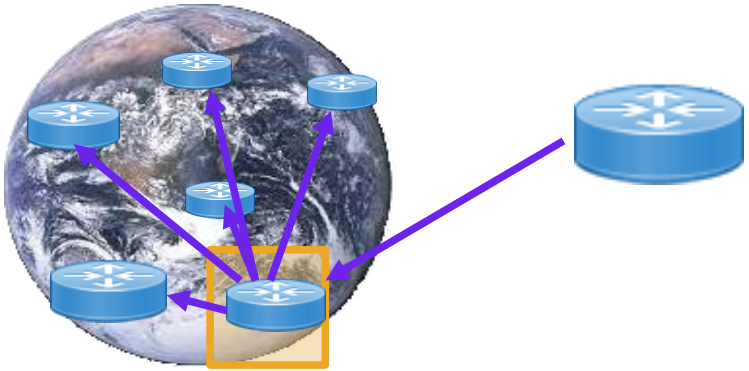
Pas exemple un trafic DDOS donc illégitime peut être arrêté en plusieurs points du réseau.

© 2021 Cisco and/or its affiliates. All rights reserved.

BGP Flowspec – RR

Les «Routes Reflectors» (RR) peuvent servir à relayer les règles à travers le système de routeurs BGP.

Note : la communication ne se fait que du contrôleur vers les clients. Il n'y a rien de prévu dans le sens inverse. Même pas pour vérifier l'état.



© 2021 Cisco and/or its affiliates. All rights reserved.

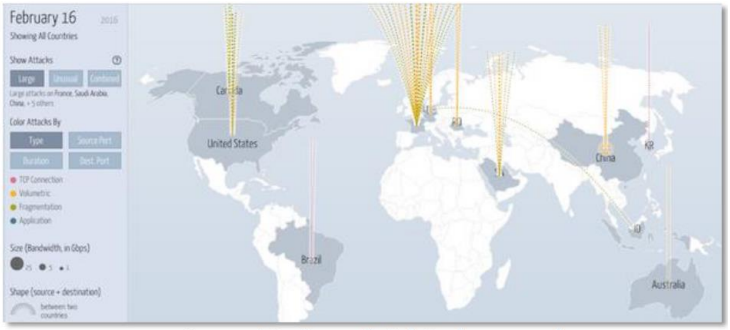
BGP Flowspec – Cas de défense contre DDOS

Lire le document BRKSPG-3012 :

Use case : DDOS mitigation

DDoS Attacks

- No longer necessary to explain the risk
  - Distributed Denial of Service (DDoS) is a lucrative activity for attackers
  - ISP, Hosting Services, Enterprises: it can jeopardize your business
    Everyone is at risk
  - 2017:
    - More sophisticated
    - Less volumetric
    - But still very high



Source: http://www.digitalattackmap.com/

© 2021 Cisco and/or its affiliates. All rights reserved.

Cisco live!

Polling Question 5

Quelle est la distance administrative d'IS-IS sur un routeur Cisco ?

1) 110
2) 115
3) 120
4) 125

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

6. IS-IS

Rappel sur IS-IS (1)

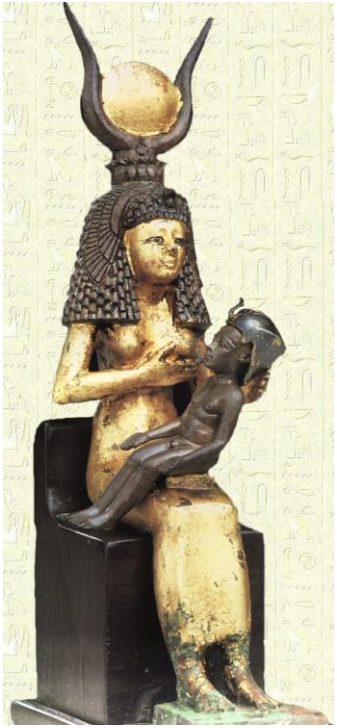
Il est très utilisé dans le domaine des télécoms et dans certaines implémentations SDN.

RFC 1195 « Use of OSI IS-IS for Routing in TCP/IP and Dual Environments »

En effet IS-IS n'est pas défini par l'IETF, mais par l'OSI : OSI Intra-Domain IS-IS Routing Protocol. Norme : ISO/CEI 10589:2002.

Pour IPv6 il y a la RFC 5308

Pour le fonctionnement IPv4/IPv6 il y a la RFC 5120



© 2021 Cisco and/or its affiliates. All rights reserved.

Rappel sur IS-IS (2)

IS-IS est un protocole très formaliste.

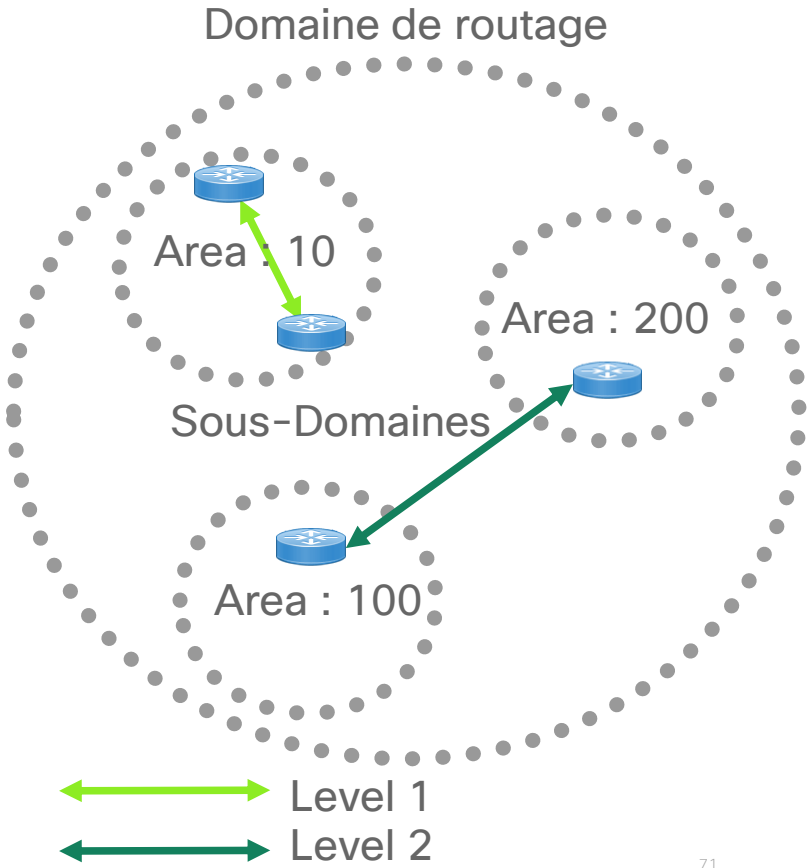
Un réseau est découpé en zone :

les «area» (aires).

Le routage intra-area est dit de niveau 1 (Level I)

Le routage inter-area est dit de niveau 2 (Level II)

Très adapté à un grand nombre de réseaux et de routeurs.

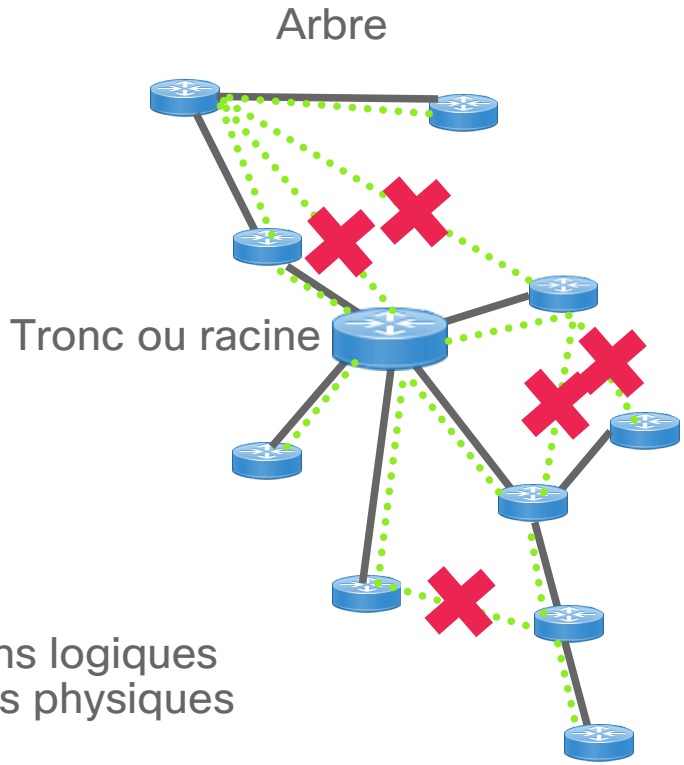


© 2021 Cisco and/or its affiliates. All rights reserved.

Rappel sur IS-IS (3)

IS-IS comme OSPF utilise Algorithme de Dijkstra (théorie des graphe) pour se représenter l'architecture du réseau et en déduire les routes.

Lire:
https://fr.wikipedia.org/wiki/Algorithme_de_Dijkstra



© 2021 Cisco and/or its affiliates. All rights reserved.

Rappel sur IS-IS (4)

Quelques définitions :

IS : Intermediate System

ES : End System

CLNS : Connectionless Network Service.

CLNP : Connectionless Network Protocol

Trois types de routeurs :

Level 1

Level 2

Level 1-2

© 2021 Cisco and/or its affiliates. All rights reserved.

Rappel sur IS-IS (5)

Configuration de base :

(voir : https://www.cisco.com/c/fr_ca/support/docs/ip/integrated-intermediate-system-to-intermediate-system-is-is/13795-is-is-ip-config.html)

```
interface loopback 0
ip address 172.16.1.1 255.255.255.255

interface FastEthernet 0
ip address 172.16.2.2 255.255.0.0
ip router isis
ipv6 address 2001:FFFF:FFFF::2/64
ipv6 enable
ipv6 router isis

router isis
passive-interface loopback0
net 49.0001.1720.1600.1001.00
```

@ loopback 0

© 2021 Cisco and/or its affiliates. All rights reserved.

Les bases : Clear text, par interface

```
interface FastEthernet 8
ip address 172.18.8.1 255.255.0.0
ip router isis
isis password mot2passe [level-1 |
level-2 ]

interface FastEthernet 9
ip address 172.19.9.9 255.255.0.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
```

```
interface FastEthernet 8
ip address 172.18.8.2 255.255.0.0
ip router isis
isis password mot2passe [level-1 |
level-2 ]

interface FastEthernet 9
ip address 172.19.9.10 255.255.0.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Les bases : Clear text, par aire (area)

```
interface FastEthernet 8
ip address 172.18.8.1 255.255.0.0
ip router isis

interface FastEthernet 9
ip address 172.19.9.9 255.255.0.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
area-password mot2passe
```

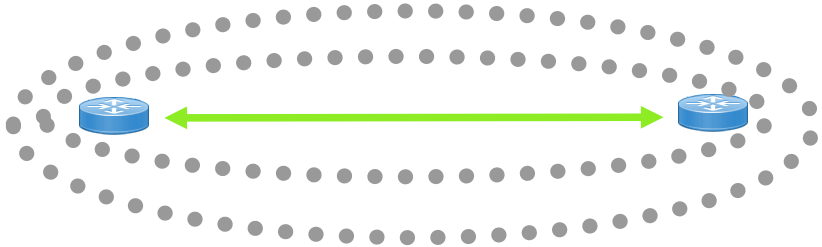
```
interface FastEthernet 8
ip address 172.18.8.2 255.255.0.0
ip router isis

interface FastEthernet 9
ip address 172.19.9.10 255.255.0.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
area-password mot2passe
```

© 2021 Cisco and/or its affiliates. All rights reserved.

Les bases : Clear text, par domaine

```
interface FastEthernet 8
ip address 172.18.8.1 255.255.0.0
ip router isis

interface FastEthernet 9
ip address 172.19.9.9 255.255.0.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00
domain-password mot2passe
```

```
interface FastEthernet 8
ip address 172.18.8.2 255.255.0.0
ip router isis

interface FastEthernet 9
ip address 172.19.9.10 255.255.0.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00
domain-password mot2passe
```



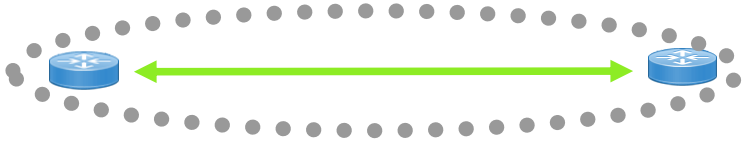
Note : Il est possible de combiner les 3 méthodes vues avant ensemble.

© 2021 Cisco and/or its affiliates. All rights reserved.

Les bases : MD5, par zone

```
key chain cisco
key 100
key-string tasman-drive
!
interface GigabitEthernet3/0/0
ip address 10.1.1.1 255.255.255.252
ip router isis real_secure_network
isis authentication mode md5 level-1
isis authentication key-chain cisco level-1
!
router isis real_secure_network
net 49.0000.0101.0101.0101.00
is-type level-1
authentication mode md5 level-1
authentication key-chain cisco level-1
!
```

Peut être mode texte ‘text’



© 2021 Cisco and/or its affiliates. All rights reserved.

Références

https://www.cisco.com/c/en/us/support/docs/ip/integrated-intermediate-system-to-intermediate-system-is-is/13792-isis-authent.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/xe-16-10/irs-xe-16-10-book/irs-scty.html

© 2021 Cisco and/or its affiliates. All rights reserved.

Conclusion

Notre civilisation est dépendante pour son fonctionnement de la bonne santé des réseaux informatiques.

L'uniformisation et la re-centralisation des réseaux (Cloud) la rende encore plus à risque.

Internet et le routage n'ont pas été prévus pour mettre en place de la sécurité, qui était inutile. Cela peut devenir une faille systémique. Faille systémique qui peut en cas d'attaque majeure renvoyer notre civilisation un siècle en arrière (et encore plutôt dans les années 1910 que 1990).

Dans ce contexte la sécurisation des réseaux est une priorité majeure.

© 2021 Cisco and/or its affiliates. All rights reserved.

Avez-vous encore des questions ?
Utilisez le panneau « Q&R »

Forum Ask Me Anything

Retrouvez notre expert sur la page de Discussion

Toutes les nouvelles questions sur le sujet de ce webinaire seront répondues par la suite jusqu'à la semaine prochaine: 29 Oct.

Postez une question ici

© 2021 Cisco and/or its affiliates. All rights reserved.

Prochains événements

22 Oct. Ask Me Anything Certifications

Certifications Cisco Trucs et Astuces CCIE CCNP CCNA

28 Oct. Community Live IPv6 Multicast

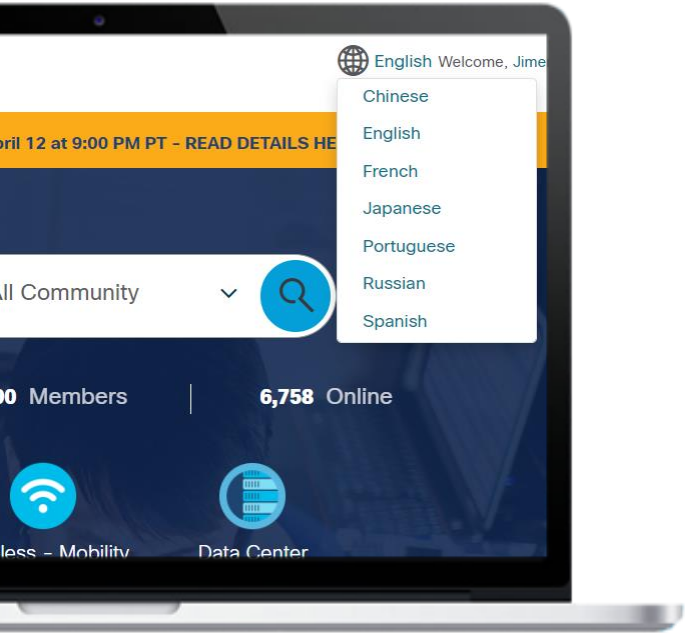
Adaptations des protocoles (composante multicast) les plus connus au format d'adressage IPv6.
Routage Multicast (MLD, PIM, M-BGP) sur réseau IPv6.

[Calendrier : Inscrivez-vous ici !]

CCIE R&S
#8935

© 2021 Cisco and/or its affiliates. All rights reserved.

Où que vous soyez restez connecté…



- Facebook CiscoSupportCommunity
- Twitter @cisco_support
- YouTube CiscoSupportChannel
- LinkedIn Cisco Community
- Instagram CiscoSupportCommunity

© 2021 Cisco and/or its affiliates. All rights reserved.


Avez-vous des commentaires ?
Répondez à notre enquête !

The bridge to possible