អត្ថប្រយោជន៍នៃ VLANs: VLANs ផ្តល់អត្ថប្រយោជន៍ជាច្រើន:

បង្កើនប្រសិទ្ធភាពបណ្តាញ: តាមរយៈការបែងចែកដែនផ្សាយ (broadcast domains) VLANs កាត់បន្ថយចរាចរណ៍ដែលមិនចាំបាច់ និងបង្កើនប្រសិទ្ធភាពបណ្តាញទាំងមូល។

បង្កើនសុវត្ថិភាព: VLANs ញែកទិន្នន័យរសើប និងការពារការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាតចំពោះធនធានបណ្តាញជាក់លាក់។

កាត់បន្ថយការចំណាយ: VLANs អាចកាត់បន្ថយតម្រូវការឧបករណ៍ routing ដែលមានតម្លៃថ្លៃដោយអនុញ្ញាតឱ្យមានការបែងចែកឡូជីខល (logical segmentation) នៅក្នុង switch តែមួយ។

ការគ្រប់គ្រងបណ្តាញងាយស្រួល: VLANs ធ្វើឱ្យវាកាន់តែងាយស្រួលក្នុងការបន្ថែម ផ្លាស់ប្តូរទីតាំង និងផ្លាស់ប្តូរឧបករណ៍បណ្តាញ និងអ្នកប្រើប្រាស់ដោយមិនចាំបាច់កំណត់រចនាសម្ព័ន្ធហេដ្ឋារចនាសម្ព័ន្ធរូបវន្តឡើងវិញ។

បង្កើនភាពបត់បែន និងអាចពង្រីកបាន: VLANs អនុញ្ញាតឱ្យមានការពង្រីក និងការរៀបចំបណ្តាញឡើងវិញបានយ៉ាងងាយស្រួលដោយគ្មានការផ្លាស់ប្តូរផ្នែករឹងធំដុំ។

តើការបែងចែក VLAN កែលម្អដំណើរការបណ្តាញ និងសុវត្ថិភាពយ៉ាងដូចម្តេច?

ដំណើរការបណ្តាញ: VLANs ធ្វើឱ្យប្រសើរឡើងនូវដំណើរការបណ្តាញដោយបំបែកដែនផ្សាយធំៗទៅជាដែនតូចៗ។ នេះកាត់បន្ថយបរិមាណចរាចរណ៍ផ្សាយ (broadcast traffic) ដែលឧបករណ៍នីមួយៗត្រូវដំណើរការ ដែលនាំឱ្យកកស្ទះបណ្តាញតិច និងប្រសិទ្ធភាពរួមប្រសើរឡើង។

សុវត្ថិភាព: VLANs បង្កើនសុវត្ថិភាពដោយញែកចរាចរណ៍រវាងក្រុមអ្នកប្រើប្រាស់ ឬឧបករណ៍ផ្សេងៗគ្នា។ នេះមានន័យថា ប្រសិនបើការបំពានសុវត្ថិភាពកើតឡើងនៅក្នុង VLAN មួយ វាមិនទំនងប៉ះពាល់ដល់ VLAN ផ្សេងទៀតទេ។ វាក៏ការពារការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាតចំពោះទិន្នន័យ និងធនធានរសើបដោយរក្សាទុកពួកវានៅលើ VLAN ដាច់ដោយឡែក។

តើមានប្រភេទ passwords អ្វីខ្លះ ប្រើក្នុងការកំណត់ securing លើ CISCO router?

Console password: ការពារការចូលប្រើដោយផ្ទាល់ទៅកាន់ router តាមរយៈ console port ។

Auxiliary password: ការពារការចូលប្រើតាមរយៈ auxiliary port (ឧទាហរណ៍ សម្រាប់ modem connections) ។

Telnet/SSH password (VTY password): ការពារការចូលប្រើពីចម្ងាយទៅកាន់ router តាមរយៈ Telnet ឬ SSH ។

Enable password/secret: ការពារការចូលប្រើទៅកាន់ privileged EXEC mode ។ enable secret ត្រូវបានណែនាំជាង enable password ព្រោះវាទុក password ជាទម្រង់អ៊ិនគ្រីប (encrypted format) ។

ចូរពន្យល់ពីភាពខុសគ្នារវាង Physical Topology ទៅនឹង Logical Topology

Physical Topology: រៀបរាប់ពីការរៀបចំជាក់ស្តែងនៃឧបករណ៍ និងខ្សែនៅក្នុងបណ្តាញ។ វាបង្ហាញពីរបៀបដែលឧបករណ៍ត្រូវបានតភ្ជាប់គ្នាជាលក្ខណៈរូបវន្ត។

Logical Topology: រៀបរាប់ពីរបៀបដែលទិន្នន័យហូរតាមបណ្តាញ ដោយមិនអាស្រ័យលើការរៀបចំរូបវន្តនោះទេ។ វាបង្ហាញពីការតភ្ជាប់ឡូជីខលរវាងឧបករណ៍ និងរបៀបដែលពួកវាទំនាក់ទំនងគ្នា។

តើអ្វីជាភាពខុសគ្នារវាង switch, hub, និង router?

Hub: ជាឧបករណ៍បណ្តាញមូលដ្ឋានដែលភ្ជាប់ឧបករណ៍ Ethernet ជាច្រើនចូលគ្នា ធ្វើឱ្យពួកវាដើរតួជាផ្នែកបណ្តាញតែមួយ។ វាដំណើរការនៅ physical layer (Layer 1) នៃម៉ូដែល OSI ហើយគ្រាន់តែផ្សាយទិន្នន័យដែលចូលមកទាំងអស់ទៅកាន់ឧបករណ៍ដែលបានតភ្ជាប់ទាំងអស់។

Switch: ជាឧបករណ៍បណ្តាញទំនើបជាងមុនដែលភ្ជាប់ឧបករណ៍ជាច្រើននៅលើបណ្តាញមូលដ្ឋាន (LAN) ។ វាដំណើរការនៅ data link layer (Layer 2) នៃម៉ូដែល OSI ហើយរៀនអាសយដ្ឋាន MAC របស់ឧបករណ៍ដែលបានតភ្ជាប់។ វាបញ្ជូនទិន្នន័យទៅកាន់អ្នកទទួលដែលបានកំណត់តែប៉ុណ្ណោះ ធ្វើឱ្យប្រសើរឡើងនូវប្រសិទ្ធភាពបណ្តាញ និងកាត់បន្ថយការប៉ះទង្គិច។

Router: ជាឧបករណ៍បណ្តាញដែលបញ្ជូនកញ្ចប់ទិន្នន័យរវាងបណ្តាញកុំព្យូទ័រផ្សេងៗគ្នា។ វាដំណើរការនៅ network layer (Layer 3) នៃម៉ូដែល OSI ហើយប្រើអាសយដ្ឋាន IP ដើម្បីកំណត់ផ្លូវល្អបំផុតសម្រាប់ទិន្នន័យក្នុងការធ្វើដំណើរ។ Routers ភ្ជាប់បណ្តាញផ្សេងៗគ្នា (ឧទាហរណ៍ បណ្តាញផ្ទះទៅកាន់អ៊ីនធឺណិត) និងអនុញ្ញាតឱ្យមានការទំនាក់ទំនងរវាងពួកវា។

និយាយពីអ្វីដែលជា រង្វាស់ នៃ EIGRP protocol? រង្វាស់ (metric) របស់ EIGRP គឺជាតម្លៃផ្សំដែលត្រូវបានគណនាដោយប្រើ bandwidth, delay, reliability, និង load ។ តាមលំនាំដើម EIGRP ប្រើតែ bandwidth និង delay សម្រាប់ការគណនារង្វាស់។ រូបមន្តគឺ: Metric = 256×(256−LoadK1×Bandwidth+K2×Bandwidth​+K3×Delay) ដែល K1, K2, K3, K4, និង K5 គឺជា K-values ដែលអាចកំណត់បាន។ តាមលំនាំដើម K1=1, K2=0, K3=1, K4=0, K5=0 ។

តើអ្វីជាភាពខុសគ្នារវាង TCP និង UDP?

TCP (Transmission Control Protocol):

Connection-oriented: បង្កើតការតភ្ជាប់មុនពេលបញ្ជូនទិន្នន័យ។

Reliable: ធានាការបញ្ជូនទិន្នន័យ បញ្ជូនកញ្ចប់ដែលបាត់បង់ឡើងវិញ និងផ្តល់ការគ្រប់គ្រងលំហូរ (flow control) និងការពិនិត្យកំហុស (error checking) ។

Ordered delivery: ធានាថាទិន្នន័យមកដល់តាមលំដាប់លំដោយត្រឹមត្រូវ។

Slower: ដោយសារតែមាន overhead សម្រាប់ការធានានូវភាពជឿជាក់។

ត្រូវបានប្រើសម្រាប់កម្មវិធីដែលទាមទារភាពជឿជាក់ខ្ពស់ ដូចជាការ Browse គេហទំព័រ (HTTP), អ៊ីមែល (SMTP), និងការផ្ទេរឯកសារ (FTP) ។

UDP (User Datagram Protocol):

Connectionless: មិនបង្កើតការតភ្ជាប់មុនពេលបញ្ជូនទិន្នន័យ។

Unreliable: មិនធានាការបញ្ជូន ការបញ្ជូនឡើងវិញ ឬការតម្រៀបលំដាប់។

Faster: មាន overhead តិចដោយសារតែខ្វះយន្តការធានាភាពជឿជាក់។

ត្រូវបានប្រើសម្រាប់កម្មវិធីដែលល្បឿនមានសារៈសំខាន់ជាងការធានាការបញ្ជូន ដូចជាការ streaming វីដេអូ/អូឌីយ៉ូ, ការលេងហ្គេមអនឡាញ, និង DNS lookups ។

គេមាន route ចំនួនពីរ: 192.168.1.0/24 and 192.168.1.0/28. របៀប configure deny 192.168.1.0/28 ហើយបន្ទាប់មក allow 192.168.1.0/24 ក្នុង EIGRP? ដើម្បីសម្រេចបាននេះ អ្នកជាធម្មតាប្រើ access control list (ACL) ហើយបន្ទាប់មកអនុវត្តវាទៅ EIGRP ដោយប្រើ distribute-list ។ ផ្លូវដែលជាក់លាក់ជាង (192.168.1.0/28) ត្រូវតែត្រូវបានបដិសេធមុនពេលផ្លូវដែលមិនសូវជាក់លាក់ (192.168.1.0/24) ត្រូវបានអនុញ្ញាត។

access-list 10 deny 192.168.1.0 0.0.0.15 // Deny 192.168.1.0/28

access-list 10 permit 192.168.1.0 0.0.0.255 // Permit 192.168.1.0/24

!

router eigrp [AS\_number]

distribute-list 10 in [interface\_type interface\_number] // To filter incoming updates

distribute-list 10 out [interface\_type interface\_number] // To filter outgoing updates

ម្យ៉ាងវិញទៀត ដោយប្រើ prefix-list (ដែលជាទូទៅត្រូវបានណែនាំសម្រាប់ការច្រោះផ្លូវ):

ip prefix-list DENY\_28\_ALLOW\_24 seq 5 deny 192.168.1.0/28

ip prefix-list DENY\_28\_ALLOW\_24 seq 10 permit 192.168.1.0/24

!

router eigrp [AS\_number]

distribute-list prefix DENY\_28\_ALLOW\_24 in [interface\_type interface\_number]

distribute-list prefix DENY\_28\_ALLOW\_24 out [interface\_type interface\_number]

តើមានអ្វីខ្លះនៃ EIGRP Tables? EIGRP រក្សាតារាងចំនួនបី:

Neighbor Table: ផ្ទុកព័ត៌មានអំពី EIGRP neighbors ដែលបានតភ្ជាប់ដោយផ្ទាល់ ដូចជាអាសយដ្ឋាន IP និងព័ត៌មាន interface របស់ពួកវា។

Topology Table: ផ្ទុកផ្លូវដែលបានរៀនទាំងអស់ពី EIGRP neighbors រួមទាំង feasible successors និង successor routes ។ វាមាន destinations ទាំងអស់ដែលត្រូវបានផ្សាយដោយ neighbors រួមជាមួយ metric របស់ពួកវា។

Routing Table: មានផ្លូវល្អបំផុតទៅកាន់ destinations ដែលស្គាល់ទាំងអស់ ដែលបានជ្រើសរើសពី topology table ។ ទាំងនេះគឺជាផ្លូវដែល router នឹងប្រើដើម្បីបញ្ជូនចរាចរណ៍។

តើអ្វីទៅ EIGRP សង្ខេបនៃ route និង EIGRP external route?

EIGRP Summary Route: ផ្លូវសង្ខេបតំណាងឱ្យផ្លូវជាក់លាក់ជាច្រើនដែលជាផ្លូវតែមួយដែលមិនសូវជាក់លាក់។ នេះជួយកាត់បន្ថយទំហំតារាង routing និងចរាចរណ៍ update routing ។ ឧទាហរណ៍ 192.168.1.0/24, 192.168.2.0/24, និង 192.168.3.0/24 អាចត្រូវបានសង្ខេបជា 192.168.0.0/22 ។

EIGRP External Route: ផ្លូវខាងក្រៅគឺជាផ្លូវដែលត្រូវបានរៀនដោយ EIGRP ពី protocol routing ផ្សេងទៀត (ឧទាហរណ៍ OSPF, RIP, BGP) ហើយបន្ទាប់មកត្រូវបាន redistribute ចូលទៅក្នុង EIGRP ។ ផ្លូវទាំងនេះត្រូវបានសម្គាល់ដោយ external flag ហើយមាន administrative distance 170 តាមលំនាំដើម ដែលបង្ហាញថាពួកវាមិនសូវត្រូវបានណែនាំជាង internal EIGRP routes ។

តើរបៀបធ្វើ redistribute លើ IPv6 default route ក្នុង EIGRP? ដើម្បី redistribute ផ្លូវ default IPv6 ចូលទៅក្នុង EIGRP អ្នកជាធម្មតាប្រើ command redistribute static (សន្មត់ថាផ្លូវ default គឺជា static route) ឬ redistribute ospf ។ល។ រួមជាមួយ command default-information originate ប្រសិនបើអ្នកចង់ឱ្យ router ផ្សាយផ្លូវ default ចូលទៅក្នុង EIGRP ។

ដំបូង ត្រូវប្រាកដថាអ្នកមានផ្លូវ default IPv6 ដែលបានកំណត់រចនាសម្ព័ន្ធនៅលើ router:

ipv6 route ::/0 [next-hop-ipv6-address or exit-interface]

បន្ទាប់មក នៅក្នុងការកំណត់រចនាសម្ព័ន្ធ router IPv6 EIGRP:

ipv6 router eigrp [AS\_number]

redistribute static

default-information originate

ការ ផ្ទុក Tables routing ក្នុង OSPF? និង សរសេរ command នៅក្នុង OSPF, routing table ត្រូវបានបំពេញដោយផ្អែកលើ Link-State Database (LSDB) ។ LSDB មាន Link State Advertisements (LSAs) ទាំងអស់ដែលត្រូវបាន flooded ពេញមួយ area ។ Routers OSPF ប្រើ algorithm Shortest Path First (SPF) របស់ Dijkstra ដើម្បីគណនាផ្លូវល្អបំផុតទៅកាន់ destinations ទាំងអស់ពី LSDB ហើយបន្ទាប់មកបំពេញ routing table ។

ដើម្បីមើល OSPF routing table (ឧទាហរណ៍ ផ្លូវ OSPF ដែលត្រូវបានដំឡើងនៅក្នុង IP routing table) អ្នកអាចប្រើ command:

show ip route ospf

ដើម្បីមើល OSPF database (LSDB) ដែលត្រូវបានប្រើដើម្បីបង្កើត routing table:

show ip ospf database

តើអ្វីទៅជាជំហានដែលត្រូវការដើម្បីផ្លាស់ប្តូរ Neighborship ទៅជា adjacency? ការផ្លាស់ប្តូរពី OSPF neighborship ទៅជា full adjacency រួមមានស្ថានភាពជាច្រើន ដែល routers ផ្លាស់ប្តូរព័ត៌មាន link-state លម្អិតបន្ថែមទៀតដើម្បីបង្កើតផែនទី topological ពេញលេញ។ ជំហាន/ស្ថានភាពសំខាន់ៗសម្រាប់ការ full adjacency គឺ:

Down: មិនទាន់ទទួលបាន Hello ពី neighbor ទេ។

Init: បានទទួល Hello ហើយ ប៉ុន្តែ Router ID របស់ router ផ្ទាល់ខ្លួនមិននៅក្នុង Hello របស់ neighbor ទេ។

2-Way: បានទទួល Hello ជាមួយនឹង Router ID ទៅវិញទៅមក (Router ID របស់ router គឺនៅក្នុង Hello របស់ neighbor) ។ នេះគឺជាកន្លែងដែលការបោះឆ្នោត DR/BDR កើតឡើងនៅលើបណ្តាញ multi-access ។

Exstart: Routers បង្កើតទំនាក់ទំនង master-slave ហើយផ្លាស់ប្តូរកញ្ចប់ DBD (Database Description) ដើម្បីរៀបរាប់ពី LSDBs របស់ពួកវា។

Exchange: Routers ផ្លាស់ប្តូរកញ្ចប់ DBD ពិតប្រាកដ។

Loading: Routers ផ្ញើកញ្ចប់ Link State Request (LSR) សម្រាប់ LSAs ដែលបាត់បង់ និងទទួលបានកញ្ចប់ Link State Update (LSU) ។

Full: LSDBs ត្រូវបានធ្វើសមកាលកម្ម ហើយ routers គឺ fully adjacent ។

ពន្យល់កម្មវិធីកំណត់ពេល OSPF (OSPF timers)? OSPF ប្រើកម្មវិធីកំណត់ពេលដើម្បីរក្សាទំនាក់ទំនង neighbor និងធានាស្ថេរភាពបណ្តាញ:

Hello Interval: ភាពញឹកញាប់ (គិតជាវិនាទី) ដែល router OSPF ផ្ញើកញ្ចប់ Hello ចេញពី interface ។ លំនាំដើមគឺ 10 វិនាទីលើបណ្តាញ broadcast និង point-to-point និង 30 វិនាទីលើបណ្តាញ non-broadcast multi-access (NBMA) ។

Dead Interval: រយៈពេល (គិតជាវិនាទី) ដែល router រង់ចាំដើម្បីទទួលបានកញ្ចប់ Hello ពី neighbor មុនពេលប្រកាសថា neighbor នោះ down ។ លំនាំដើមគឺ 4 ដងនៃ Hello interval (40 វិនាទីសម្រាប់ broadcast/point-to-point, 120 វិនាទីសម្រាប់ NBMA) ។

Wait Timer: ប្រើក្នុងដំណើរការបោះឆ្នោត DR/BDR, កម្មវិធីកំណត់ពេលនេះស្មើនឹង Dead Interval ។

LSA Max Age Timer: អាយុកាលអតិបរមាដែល LSA អាចស្ថិតនៅក្នុង LSDB (3600 វិនាទី ឬ 1 ម៉ោង) ។ ប្រសិនបើ LSA ឈានដល់អាយុកាលអតិបរមា វានឹងត្រូវបាន flushed ចេញពី database លុះត្រាតែវាត្រូវបាន refreshed ។

ចូរ configure default និង static route នៃ IPv6 ដូចរូបខាងក្រោម៖ ដើម្បីកំណត់រចនាសម្ព័ន្ធ PC0 ឱ្យស្គាល់ PC1 និង PC1 ឱ្យស្គាល់ PC0 អ្នកត្រូវកំណត់រចនាសម្ព័ន្ធអាសយដ្ឋាន IPv6 និង routing លើ routers ទាំងអស់ (Router0, Router1, Router2, Router3) និង PC ។ អ្នកនឹងត្រូវរៀបចំ static routes សម្រាប់ការតភ្ជាប់រវាង subnets ហើយបន្ទាប់មក default route លើ edge routers (Router0 និង Router3) ដែលចង្អុលទៅ core ។

ការកំណត់រចនាសម្ព័ន្ធ Router0 (ឧទាហរណ៍មួយផ្នែកសម្រាប់ interfaces និង default route):

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:2002::1/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:002::1/64

no shutdown

!

ipv6 route ::/0 2001:B77:EF01:2002::2 // Default route pointing to Router1

ការកំណត់រចនាសម្ព័ន្ធ Router1 (ឧទាហរណ៍មួយផ្នែកសម្រាប់ interfaces និង static routes):

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:2002::2/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:222::1/64

no shutdown

!

ipv6 route 2001:B77:EF01:1002::/64 2001:B77:EF01:222::2 // Static route to Router2's subnet

ipv6 route 2001:B77:EF01:100::/64 2001:B77:EF01:222::2 // Static route to PC1's subnet

ipv6 route 2001:B77:EF01:002::/64 Null0 // Static route for connected network (or redistribute connected)

ការកំណត់រចនាសម្ព័ន្ធ Router2 (ឧទាហរណ៍មួយផ្នែកសម្រាប់ interfaces និង static routes):

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:222::2/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:1002::1/64

no shutdown

!

ipv6 route 2001:B77:EF01:002::/64 2001:B77:EF01:222::1 // Static route to PC0's subnet

ipv6 route 2001:B77:EF01:100::/64 2001:B77:EF01:1002::2 // Static route to PC1's subnet

ការកំណត់រចនាសម្ព័ន្ធ Router3 (ឧទាហរណ៍មួយផ្នែកសម្រាប់ interfaces និង default route):

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:1002::2/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:100::1/64

no shutdown

!

ipv6 route ::/0 2001:B77:EF01:1002::1 // Default route pointing to Router2

ការកំណត់រចនាសម្ព័ន្ធ PC0 (អាសយដ្ឋាន IPv6 និង Gateway):

IPv6 Address: 2001:B77:EF01:002::100

Default Gateway: 2001:B77:EF01:002::1

ការកំណត់រចនាសម្ព័ន្ធ PC1 (អាសយដ្ឋាន IPv6 និង Gateway):

IPv6 Address: 2001:B77:EF01:100::100

Default Gateway: 2001:B77:EF01:100::1

ចូរសសេរ ទំរងពេញលេញនៃ IPv6 និងបំពេញតារាង (global routing, subnet ID, Interface ID):

|  |  |  |  |
| --- | --- | --- | --- |
| ទម្រង់ពេញលេញនៃអាសយដ្ឋាន IPv6 | Global ID | Subnet ID | Interface ID |
| 2001:0BD8:0AA1:0BBA:0000:0000:0000:00A1 | 2001:BD8:0AA1:BBA | 0000 (implied) | 0000:0000:0000:00A1 |
| 2001:0BD7:0B11:00BA:0006:0000:010A:00AA | 2001:BD7:0B11 | 00BA | 0006:0000:010A:00AA |
| 2001:BBAB:0768:00EA:01F4:0000:0000:0000 | 2001:BBAB:768 | 00EA | 01F4:0000:0000:0000 |

Export to Sheets

ចំណាំ: "Global ID" ជាធម្មតាសំដៅទៅលើ global routing prefix (48 bits ដំបូង ឬ 3 hextets ដំបូងក្នុងការចាត់តាំងធម្មតា) ។ "Subnet ID" គឺជា 16 bits បន្ទាប់ ហើយ "Interface ID" គឺជា 64 bits ចុងក្រោយ។

ចូរបំពេញនឹងសំនួរខាងក្រាម (Configure DHCP and Static/EIGRP IP route on Router1, Router2, and Router3 for NET 200, NET 201, and NET 202 and ensure all computers can communicate):

ផ្នែក A: Configure DHCP

Router1 (សម្រាប់ NET 200)

ip dhcp excluded-address 192.168.200.1 192.168.200.99

ip dhcp excluded-address 192.168.200.254

ip dhcp pool NET200\_POOL

network 192.168.200.0 255.255.255.0

default-router 192.168.200.254

Router2 (សម្រាប់ NET 201)

ip dhcp excluded-address 192.168.201.1 192.168.201.99

ip dhcp excluded-address 192.168.201.254

ip dhcp pool NET201\_POOL

network 192.168.201.0 255.255.255.0

default-router 192.168.201.254

Router3 (សម្រាប់ NET 202)

ip dhcp excluded-address 192.168.202.1 192.168.202.99

ip dhcp excluded-address 192.168.202.254

ip dhcp pool NET202\_POOL

network 192.168.202.0 255.255.255.0

default-router 192.168.202.254

ផ្នែក B: Configure Static និង EIGRP IP routes ចំណាំ: ដើម្បីឱ្យកុំព្យូទ័រទាំងអស់ស្គាល់គ្នាទៅវិញទៅមក អ្នកនឹងត្រូវការ static routes សម្រាប់ការតភ្ជាប់ដោយផ្ទាល់រវាង routers និង EIGRP ដើម្បីរៀនផ្លូវទៅកាន់បណ្តាញផ្សេងទៀតដោយស្វ័យប្រវត្តិ។

Router1:

! Interface configurations based on the diagram

interface GigabitEthernet0/0

ip address 192.168.200.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 192.168.111.254 255.255.255.252

no shutdown

!

ip route 192.168.112.0 255.255.255.252 192.168.111.253 // Static route to NET 112 via Router2

ip route 192.168.201.0 255.255.255.0 192.168.111.253 // Static route to NET 201 via Router2

ip route 192.168.202.0 255.255.255.0 192.168.111.253 // Static route to NET 202 via Router2

!

router eigrp 100 // Example AS number

network 192.168.200.0 0.0.0.255

network 192.168.111.0 0.0.0.3

no auto-summary

Router2:

! Interface configurations based on the diagram

interface GigabitEthernet0/0

ip address 192.168.201.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 192.168.111.253 255.255.255.252

no shutdown

interface Serial0/0/1

ip address 192.168.112.254 255.255.255.252

no shutdown

!

ip route 192.168.200.0 255.255.255.0 192.168.111.254 // Static route to NET 200 via Router1

ip route 192.168.202.0 255.255.255.0 192.168.112.253 // Static route to NET 202 via Router3

!

router eigrp 100

network 192.168.201.0 0.0.0.255

network 192.168.111.0 0.0.0.3

network 192.168.112.0 0.0.0.3

no auto-summary

Router3:

! Interface configurations based on the diagram

interface GigabitEthernet0/0

ip address 192.168.202.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 192.168.112.253 255.255.255.252

no shutdown

!

ip route 192.168.111.0 255.255.255.252 192.168.112.254 // Static route to NET 111 via Router2

ip route 192.168.200.0 255.255.255.0 192.168.112.254 // Static route to NET 200 via Router2

ip route 192.168.201.0 255.255.255.0 192.168.112.254 // Static route to NET 201 via Router2

!

router eigrp 100

network 192.168.202.0 0.0.0.255

network 192.168.112.0 0.0.0.3

no auto-summary

តើ multicast address ប្រើក្នុង OSPF? OSPF ប្រើ multicast addresses ជាក់លាក់ដើម្បីទំនាក់ទំនងជាមួយ OSPF routers ផ្សេងទៀត:

224.0.0.5 (All OSPF Routers): អាសយដ្ឋាននេះត្រូវបានប្រើដោយ OSPF routers ដើម្បីផ្ញើកញ្ចប់ Hello និង Link State Updates (LSUs) ទៅកាន់ OSPF routers ទាំងអស់នៅលើ segment ។

224.0.0.6 (All Designated Routers - DRs and BDRs): អាសយដ្ឋាននេះត្រូវបានប្រើដោយ OSPF Designated Routers (DRs) និង Backup Designated Routers (BDRs) ដើម្បីផ្ញើ LSUs ទៅកាន់ OSPF routers ផ្សេងទៀតទាំងអស់នៅលើ multi-access segment ។ Routers ដែលមិនមែនជា DR/BDR ក៏ផ្ញើ LSUs របស់ពួកវាទៅអាសយដ្ឋាននេះផងដែរ។

តើអ្វីទៅ Static Route? និង ឧទាហរណ៍ command line

Static Route: ផ្លូវដែលត្រូវបានកំណត់រចនាសម្ព័ន្ធដោយដៃនៅក្នុង routing table របស់ router ដែលបញ្ជាក់ផ្លូវថេរសម្រាប់ចរាចរណ៍បណ្តាញដើម្បីទៅដល់ destination ជាក់លាក់មួយ។ មិនដូច dynamic routes ទេ static routes មិនសម្របខ្លួនដោយស្វ័យប្រវត្តិទៅនឹងការផ្លាស់ប្តូរបណ្តាញទេ។

ឧទាហរណ៍ command line:

ip route [destination-network] [subnet-mask] [next-hop-ip-address | exit-interface] [administrative-distance]

ឧទាហរណ៍:

ip route 192.168.10.0 255.255.255.0 10.0.0.1

command នេះប្រាប់ router ថាដើម្បីទៅដល់បណ្តាញ 192.168.10.0/24 វានឹងត្រូវបញ្ជូនកញ្ចប់ទៅកាន់អាសយដ្ឋាន IP next-hop 10.0.0.1 ។

តើអ្វីទៅ Default Route?

Default Route: ផ្លូវដែលបញ្ជាក់ផ្លូវសម្រាប់ចរាចរណ៍ទាំងអស់ដែលមិនមានផ្លូវជាក់លាក់ជាងនេះនៅក្នុង routing table ។ វាត្រូវបានគេហៅជាញឹកញាប់ថា "gateway of last resort" ហើយត្រូវបានប្រើជាទូទៅដើម្បីបញ្ជូនចរាចរណ៍ទៅកាន់អ៊ីនធឺណិត ឬទៅកាន់ core router នៅក្នុង stub network ។

ឧទាហរណ៍ command line:

ip route 0.0.0.0 0.0.0.0 [next-hop-ip-address | exit-interface]

ឧទាហរណ៍:

ip route 0.0.0.0 0.0.0.0 203.0.113.1

command នេះបញ្ជូនចរាចរណ៍ទាំងអស់ដែលមិនត្រូវបាន routed ទៅកាន់អាសយដ្ឋាន IP next-hop 203.0.113.1 ។

តើអ្វីទៅ Routing Information Protocol (RIP)? និង ឧទាហរណ៍ command line

Routing Information Protocol (RIP): ជា distance-vector routing protocol ដែលប្រើ hop count ជា metric របស់វា។ វាគឺជា protocol routing មួយក្នុងចំណោម protocol ចាស់បំផុត។ RIP ត្រូវបានប្រើជាទូទៅនៅក្នុងបណ្តាញតូចទៅមធ្យមដោយសារតែភាពសាមញ្ញរបស់វា ប៉ុន្តែវាមានដែនកំណត់ដូចជា maximum hop count 15 (16 គឺគ្មានកំណត់/មិនអាចទៅដល់បាន) និង slow convergence ។

ឧទាហរណ៍ command line (RIPv2):

router rip

version 2

network 192.168.1.0

network 10.0.0.0

no auto-summary

ចូរពន្យល់ពី User EXEC mode User EXEC mode គឺជាកម្រិតចូលប្រើដំបូងដែលអ្នកប្រើប្រាស់ទទួលបាននៅពេលចូលទៅក្នុងឧបករណ៍ Cisco ។ វាផ្តល់នូវសំណុំ commands ដែលមានកំណត់ខ្លាំងណាស់ ភាគច្រើនសម្រាប់ការត្រួតពិនិត្យមូលដ្ឋាន និងការធ្វើតេស្តការតភ្ជាប់ (ឧទាហរណ៍ ping, traceroute) ។ prompt ជាធម្មតាបញ្ចប់ដោយ > ។ អ្នកមិនអាចធ្វើការផ្លាស់ប្តូរការកំណត់រចនាសម្ព័ន្ធណាមួយនៅក្នុង mode នេះបានទេ។

ចូរពន្យល់ពី Privileged EXEC mode Privileged EXEC mode (ត្រូវបានគេស្គាល់ផងដែរថាជា enable mode) ផ្តល់ការចូលប្រើ commands របស់ router ទាំងអស់ រួមទាំង commands សម្រាប់មើលព័ត៌មានប្រព័ន្ធ debugging និង testing ។ វាត្រូវបានចូលប្រើពី User EXEC mode ដោយវាយ enable និងបញ្ចូល enable password/secret ។ prompt ជាធម្មតាបញ្ចប់ដោយ # ។ ពី mode នេះ អ្នកអាចចូលទៅ global configuration mode ។

ចូរពន្យល់ពី Global configuration mode Global configuration mode គឺជាកន្លែងដែលអ្នកធ្វើការផ្លាស់ប្តូរដែលប៉ះពាល់ដល់ប្រតិបត្តិការ router ទាំងមូល។ អ្នកចូលទៅ mode នេះពី privileged EXEC mode ដោយវាយ configure terminal ។ prompt ផ្លាស់ប្តូរទៅជា (config)# ។ ពី global configuration mode អ្នកអាចចូលទៅ sub-configuration modes ផ្សេងៗ (ឧទាហរណ៍ interface configuration mode, router configuration mode) ។

តើអ្វីទៅ IPv6? លក្ខណៈទូរទៅ របស់វា។

IPv6 (Internet Protocol version 6): គឺជាកំណែចុងក្រោយបំផុតនៃ Internet Protocol ដែលត្រូវបានរចនាឡើងដើម្បីជំនួស IPv4 ។ វាដោះស្រាយបញ្ហាការខ្វះខាតអាសយដ្ឋាន IPv4 និងណែនាំការកែលម្អជាច្រើន។

លក្ខណៈទូទៅ:

Larger Address Space: ប្រើអាសយដ្ឋាន 128-bit ដែលផ្តល់ចំនួនអាសយដ្ឋានពិសេសៗច្រើនជាងយ៉ាងសម្បើមបើធៀបនឹងអាសយដ្ឋាន 32-bit របស់ IPv4 ។

Simplified Header: មានទម្រង់ header ដែលសាមញ្ញ និងមានប្រសិទ្ធភាពជាង ដែលអាចបង្កើនប្រសិទ្ធភាព routing ។

No Broadcasts: ជំនួស broadcast ដោយ multicast និង anycast ដែលកាត់បន្ថយចរាចរណ៍បណ្តាញ។

Improved Security: IPSec ត្រូវបានបង្កើតឡើងដោយធម្មជាតិទៅក្នុង IPv6 ដែលផ្តល់សុវត្ថិភាព end-to-end (authentication និង encryption) ។

Stateless Autoconfiguration (SLAAC): អនុញ្ញាតឱ្យឧបករណ៍កំណត់រចនាសម្ព័ន្ធអាសយដ្ឋាន IPv6 របស់ពួកវាដោយស្វ័យប្រវត្តិដោយគ្មាន DHCP server ។

Better Support for Mobile IP: ត្រូវបានរចនាឡើងដោយគិតពី mobility ។

Enhanced QoS: ការគាំទ្រប្រសើរឡើងសម្រាប់ Quality of Service តាមរយៈ Flow Label field ។

តើជាអ្វី OSPF Router ID? OSPF Router ID (RID) គឺជាតម្លៃ 32-bit (format ដូចអាសយដ្ឋាន IPv4) ដែលកំណត់អត្តសញ្ញាណតែមួយគត់របស់ router OSPF នៅក្នុង OSPF autonomous system ។ វាត្រូវបានប្រើនៅក្នុង OSPF Hello packets និងនៅក្នុង Link State Advertisements (LSAs) ដើម្បីកំណត់អត្តសញ្ញាណ router ដែលមានប្រភព។ Router ID ត្រូវបានកំណត់តាមលំដាប់លំដោយដូចខាងក្រោម:

កំណត់រចនាសម្ព័ន្ធដោយដៃដោយប្រើ command router-id នៅក្រោម OSPF router configuration mode ។

អាសយដ្ឋាន IP ខ្ពស់បំផុតនៃ loopback interface ណាមួយដែល up/up ។

អាសយដ្ឋាន IP ខ្ពស់បំផុតនៃ physical interface សកម្មណាមួយដែល up/up ។

តើអ្វីទៅ RIP routing protocol? និង ឧទាហរណ៍ command line

RIP (Routing Information Protocol): (បានគ្របដណ្តប់រួចហើយនៅក្នុងសំណួរទី 21) ។

ឧទាហរណ៍ command line (RIPv2): (បានគ្របដណ្តប់រួចហើយនៅក្នុងសំណួរទី 21) ។

តើអ្វីទៅ OSPF Routing protocol? OSPF (Open Shortest Path First) គឺជា link-state routing protocol ដែលត្រូវបានប្រើប្រាស់យ៉ាងទូលំទូលាយនៅក្នុងបណ្តាញសាជីវកម្មធំៗ។ វាប្រើ algorithm របស់ Dijkstra ដើម្បីគណនាផ្លូវខ្លីបំផុតទៅកាន់ destination នីមួយៗដោយផ្អែកលើ metric "cost" ដែលត្រូវបានកំណត់ទៅ links ។ OSPF ត្រូវបានគេស្គាល់ថាសម្រាប់ការ converge លឿន ការគាំទ្រសម្រាប់ការរចនាជាឋានានុក្រម (areas) និង scalability ។

ចូរនិយាយពីលក្ខណៈមួយចំនួនរបស់ OSPF។ លក្ខណៈមួយចំនួនរបស់ OSPF រួមមាន:

Link-State Protocol: OSPF routers ផ្លាស់ប្តូរ link-state advertisements (LSAs) ដើម្បីបង្កើតផែនទី topological ពេញលេញនៃបណ្តាញ។

Hierarchical Design (Areas): គាំទ្រការបែងចែកបណ្តាញធំមួយទៅជា areas តូចៗ និងងាយស្រួលគ្រប់គ្រង ដែលបង្កើន scalability និងកាត់បន្ថយទំហំ routing table ។

Fast Convergence: សម្របខ្លួនយ៉ាងរហ័សទៅនឹងការផ្លាស់ប្តូរបណ្តាញដោយប្រើ triggered updates និង SPF algorithm ។

Cost-Based Metric: ប្រើ metric cost (bandwidth តាមលំនាំដើម) ដើម្បីកំណត់ផ្លូវល្អបំផុត។

Classless: គាំទ្រ Variable Length Subnet Masks (VLSM) និង Classless Inter-Domain Routing (CIDR) ។

Multicast Updates: ប្រើ multicast addresses (224.0.0.5 និង 224.0.0.6) សម្រាប់ការ updates ។

Authentication: គាំទ្រ clear-text និង MD5 authentication សម្រាប់ការ updates routing ប្រកបដោយសុវត្ថិភាព។

តើអ្វីទៅជាតម្រូវការសម្រាប់ការបែងចែកប្រព័ន្ធស្វយ័តទៅជាតំបន់ (area) ផ្សេងៗ? តម្រូវការចម្បងសម្រាប់ការបែងចែក autonomous system OSPF ទៅជា areas គឺដើម្បីបង្កើន scalability កាត់បន្ថយទំហំ routing table លើ routers ដែលមិនមែនជា backbone កំណត់ផលប៉ះពាល់នៃភាពមិនស្ថិតស្ថេរនៃបណ្តាញ (link flaps) និងកាត់បន្ថយភាពញឹកញាប់នៃការគណនា SPF ។ Area នីមួយៗត្រូវតែមាន router ដែលតភ្ជាប់ទៅ backbone area (Area 0) ដែលត្រូវបានគេស្គាល់ថាជា Area Border Router (ABR) ។ Area មិនមែន backbone ទាំងអស់ត្រូវតែតភ្ជាប់ដោយផ្ទាល់ទៅ backbone area ។

តើអ្វីទៅជាអត្ថប្រយោជន៍នៃការបែងចែកបណ្តាញទាំងមូលទៅជាតំបន់ (network into areas)? អត្ថប្រយោជន៍នៃការបែងចែកបណ្តាញទៅជា OSPF areas រួមមាន:

កាត់បន្ថយការគណនា SPF: ការផ្លាស់ប្តូរ link-state នៅក្នុង area មួយមិនបង្កឱ្យមានការគណនា SPF ឡើងវិញនៅក្នុង areas ផ្សេងទៀតទេ ដែលកំណត់ផលប៉ះពាល់នៃការផ្លាស់ប្តូរ topology ។

តារាង routing តូចជាងមុន: Routers នៅក្នុង non-backbone areas ត្រូវការតែព័ត៌មានលម្អិតអំពី area ផ្ទាល់ខ្លួនរបស់ពួកវា និង summary routes សម្រាប់ areas ផ្សេងទៀត ដែលកាត់បន្ថយការប្រើប្រាស់ memory ។

កាត់បន្ថយ LSA Flooding: LSAs ត្រូវបានកំណត់នៅក្នុង areas រៀងៗខ្លួន ដែលកាត់បន្ថយបរិមាណចរាចរណ៍ routing ។

បង្កើន Scalability: អនុញ្ញាតឱ្យ OSPF អាចពង្រីកទៅបណ្តាញធំៗបាន។

ការដោះស្រាយបញ្ហាងាយស្រួលជាងមុន: បញ្ហាបណ្តាញអាចត្រូវបានញែកដាច់ពីគ្នាទៅ areas ជាក់លាក់ ដែលធ្វើឱ្យការដោះស្រាយបញ្ហាកាន់តែងាយស្រួល។

តើជាអ្វី Backbone Area? Backbone Area ត្រូវបានគេស្គាល់ផងដែរថាជា Area 0 (ឬ Area 0.0.0.0) គឺជា area កណ្តាល និងសំខាន់បំផុតក្នុងការរចនាឋានានុក្រម OSPF ។ Area មិនមែន backbone ផ្សេងទៀតទាំងអស់ត្រូវតែតភ្ជាប់ទៅ backbone area ។ តួនាទីចម្បងរបស់ backbone គឺផ្តល់ផ្លូវចែកចាយឡូជីខល និងរូបវន្តសម្រាប់ព័ត៌មាន routing រវាង areas ។

តើប៉ារ៉ាម៉ែត្រ (Parameters) អ្វីខ្លះដែលត្រូវគ្នាសម្រាប់ប៉ោតទ័រពីរដើម្បីក្លាយជាអ្នកជិតខាង (two routers to become neighbors)? សម្រាប់ routers OSPF ពីរដើម្បីក្លាយជា neighbors (ហើយទីបំផុតឈានដល់ full adjacency) ប៉ារ៉ាម៉ែត្រខាងក្រោមត្រូវតែត្រូវគ្នានៅលើ segment ដែលចែករំលែករបស់ពួកវា:

Hello Interval: ភាពញឹកញាប់ដែលកញ្ចប់ Hello ត្រូវបានផ្ញើ។

Dead Interval: រយៈពេលដែល router រង់ចាំមុនពេលប្រកាសថា neighbor down ។

Area ID: OSPF area ដែល interface ជាកម្មសិទ្ធិ។

Authentication Type and Password (ប្រសិនបើបានកំណត់រចនាសម្ព័ន្ធ): ប្រសិនបើ authentication ត្រូវបានបើក នោះប្រភេទ (ឧទាហរណ៍ clear text, MD5) និង password ត្រូវតែត្រូវគ្នា។

Stub Area Flag (ប្រសិនបើបានកំណត់រចនាសម្ព័ន្ធ): ប្រសិនបើ area ត្រូវបានកំណត់រចនាសម្ព័ន្ធជា stub area នោះ flag នេះត្រូវតែត្រូវគ្នា។

Subnet Mask (លើ broadcast/non-broadcast links): សម្រាប់ point-to-point links, subnet mask មិនចាំបាច់ត្រូវគ្នាទេ ប៉ុន្តែសម្រាប់ multi-access segments ពួកវាត្រូវតែត្រូវគ្នាសម្រាប់ការតភ្ជាប់ IP និងការរកឃើញ neighbor ។

ពន្យល់ពី OSPF states? (បានគ្របដណ្តប់រួចហើយនៅក្នុងសំណួរទី 13 អំពីជំហានទៅ adjacency) ។

ពន្យល់ OSPF LSA, LSU និង LSR?

LSA (Link State Advertisement): កញ្ចប់តូចមួយនៃព័ត៌មាន routing ដែលរៀបរាប់ពីស្ថានភាពនៃ links (interfaces) របស់ router និងបណ្តាញដែលពាក់ព័ន្ធ។ LSAs ត្រូវបានបង្កើតដោយ OSPF routers និង flooded ពេញមួយ area ដើម្បីបង្កើត Link-State Database (LSDB) ។ មាន LSAs ជាច្រើនប្រភេទ (ឧទាហរណ៍ Router LSA, Network LSA, Summary LSA) ។

LSU (Link State Update): កញ្ចប់ដែលមាន LSAs មួយឬច្រើន។ LSUs ត្រូវបានប្រើដើម្បី reliably flood LSAs ពេញ OSPF area ។ នៅពេលដែល router ទទួលបាន LSU វានឹង acknowledge វា និង update LSDB របស់វា។

LSR (Link State Request): កញ្ចប់ដែលត្រូវបានផ្ញើដោយ OSPF router នៅពេលដែលវារកឃើញថាផ្នែកខ្លះនៃ LSDB របស់វាហួសសម័យ ឬមិនពេញលេញបើប្រៀបធៀបទៅនឹង neighbor របស់វា។ LSR ស្នើសុំ LSAs ជាក់លាក់ពី neighbor ដើម្បីធ្វើសមកាលកម្ម LSDBs ។

តើអ្វីទៅជាជំហានដែលត្រូវការដើម្បីផ្លាស់ប្តូរ Neighborship ទៅជា adjacency? (បានគ្របដណ្តប់រួចហើយនៅក្នុងសំណួរទី 13) ។

តើជាអ្វី default Hello Interval? Default Hello Interval សម្រាប់ OSPF គឺ:

10 វិនាទី: លើបណ្តាញ broadcast multi-access (ដូចជា Ethernet) និង point-to-point links ។

30 វិនាទី: លើបណ្តាញ non-broadcast multi-access (NBMA) (ដូចជា Frame Relay, ATM) ។

តើជាអ្វី default Dead Interval? Default Dead Interval សម្រាប់ OSPF ជាធម្មតាគឺបួនដងនៃ Hello Interval:

40 វិនាទី: លើបណ្តាញ broadcast multi-access និង point-to-point links ។

120 វិនាទី: លើបណ្តាញ non-broadcast multi-access (NBMA) ។

តើ OSPF LSA មានប្រភេទអ្វីខ្លះ? មានប្រភេទ OSPF LSAs ជាច្រើន ដែលនីមួយៗមានព័ត៌មាន routing ជាក់លាក់:

Type 1 - Router LSA (Router Link Advertisements): បង្កើតដោយ router នីមួយៗនៅក្នុង area ដោយរៀបរាប់ពីស្ថានភាពនៃ links (interfaces) របស់វាទៅកាន់ routers ផ្សេងទៀត និងបណ្តាញនៅក្នុង area តែមួយ។ Flooded តែនៅក្នុង area របស់វាប៉ុណ្ណោះ។

Type 2 - Network LSA (Network Link Advertisements): បង្កើតដោយ Designated Router (DR) នៅលើបណ្តាញ multi-access ដោយរៀបរាប់ពី routers ដែលបានតភ្ជាប់ទៅ segment នោះ។ Flooded តែនៅក្នុង area របស់វាប៉ុណ្ណោះ។

Type 3 - Summary LSA (Inter-Area Link Advertisements): បង្កើតដោយ Area Border Routers (ABRs) ដើម្បីផ្សាយផ្លូវពី area មួយទៅ area មួយទៀត។ ប្រើសម្រាប់ការ routing រវាង areas ។

Type 4 - ASBR Summary LSA: បង្កើតដោយ ABRs ដើម្បីផ្សាយទីតាំងរបស់ Autonomous System Boundary Router (ASBR) ទៅ areas ផ្សេងទៀត។

Type 5 - External LSA (AS External Link Advertisements): បង្កើតដោយ ASBRs ដើម្បីផ្សាយផ្លូវដែលបានរៀនពី protocol routing ផ្សេងទៀត (external routes) ចូលទៅក្នុង OSPF ។ Flooded ពេញ areas ទាំងអស់ (លើកលែងតែ stub/NSSA areas) ។

Type 7 - NSSA External LSA: បង្កើតដោយ ASBR នៅក្នុង Not So Stubby Area (NSSA) ដើម្បីផ្សាយ external routes ចូលទៅក្នុង NSSA ។ LSAs ប្រភេទ 7 ទាំងនេះត្រូវបានបំប្លែងទៅជា LSAs ប្រភេទ 5 ដោយ NSSA ABR នៅពេលបញ្ជូនទៅ areas ផ្សេងទៀត។

ចូរធ្វើការ configure OSPF Routing Protocol? ការកំណត់រចនាសម្ព័ន្ធ OSPF មូលដ្ឋានរួមមានការបើកដំណើរការ OSPF process ការកំណត់បណ្តាញដែលត្រូវផ្សាយ និងការចាត់តាំងពួកវាទៅ area មួយ។

router ospf [process-id]

router-id [x.x.x.x] // (Optional, but recommended)

network [network-address] [wildcard-mask] area [area-id]

// ឧទាហរណ៍: network 192.168.1.0 0.0.0.255 area 0

// ឧទាហរណ៍: network 10.0.0.0 0.255.255.255 area 1

passive-interface [interface-type interface-number] // (Optional, to suppress OSPF on an interface)

តើ EIGRP ត្រូវការទេ “ip default-network" command អោយដំណើរការ default route? ទេ EIGRP ជាទូទៅមិនត្រូវការ command ip default-network ដើម្បីផ្សាយ default route ទេ។ ខណៈពេលដែល ip default-network ត្រូវបានប្រើនៅក្នុង EIGRP/IGRP ចាស់ វិធីសាស្ត្រដែលត្រូវបានណែនាំដើម្បី inject default route ចូលទៅក្នុង EIGRP គឺដោយប្រើ command redistribute static (ប្រសិនបើ static default route មាន) ឬ ip summary-address eigrp [AS\_number] 0.0.0.0 0.0.0.0 នៅលើ interface មួយ។ Command default-information originate ក៏អាចត្រូវបានប្រើផងដែរ ជាពិសេសនៅពេល redistribute ពី protocol ផ្សេងទៀត ឬបង្កើត default route ដោយផ្អែកលើ external source ។

តើខ្ញុំគួរប្រើវាជាមួយ eigrp log-neighbor-changes command នៅពេលដែលខ្ញុំតំឡើង EIGRP? Command eigrp log-neighbor-changes បើកដំណើរការ logging នៃការផ្លាស់ប្តូរស្ថានភាព neighbor EIGRP (ឧទាហរណ៍ neighbor ឡើង ឬចុះ) ។ ជាទូទៅ វាត្រូវបានណែនាំឱ្យប្រើ command នេះ ជាពិសេសក្នុងអំឡុងពេលដំឡើងដំបូង និងនៅក្នុងបរិស្ថានផលិតកម្ម។ វាផ្តល់ព័ត៌មានដោះស្រាយបញ្ហាដែលមានតម្លៃដោយបង្ហាញនៅពេលដែល neighbor adjacencies ត្រូវបានបង្កើត ឬបាត់បង់ ដែលអាចជួយវិនិច្ឆ័យបញ្ហាការតភ្ជាប់ ឬ links ដែលមិនស្ថិតស្ថេរ។

តើ EIGRP support secondary addresses? បាទ EIGRP គាំទ្រ secondary IP addresses ។ ប្រសិនបើ interface មាន secondary IP address ដែលបានកំណត់រចនាសម្ព័ន្ធ EIGRP នឹងផ្សាយបណ្តាញដែលពាក់ព័ន្ធនឹង secondary address នោះ។ នេះអាចមានប្រយោជន៍ក្នុងសេណារីយ៉ូដែលអ្នកត្រូវការ IP subnets ជាច្រើននៅលើ physical interface តែមួយ។

តើ EIGRP មានសមត្ថភាព debugging អ្វីខ្លះ? EIGRP ផ្តល់ commands debugging ជាច្រើនដើម្បីត្រួតពិនិត្យប្រតិបត្តិការរបស់វា និងដោះស្រាយបញ្ហា។ commands debugging EIGRP ទូទៅមួយចំនួនរួមមាន:

debug eigrp packets: បង្ហាញសកម្មភាពកញ្ចប់ EIGRP (Hello, Update, Query, Reply, Ack) ។

debug eigrp neighbor: បង្ហាញព័ត៌មានអំពីការផ្លាស់ប្តូរស្ថានភាព neighbor EIGRP ។

debug ip eigrp: command debug ទូទៅជាងមុនដែលអាចរួមបញ្ចូលព្រឹត្តិការណ៍ EIGRP ផ្សេងៗ។

debug eigrp internal: ផ្តល់ព័ត៌មានលម្អិតអំពី internal EIGRP processes ។

debug eigrp event: បង្ហាញព្រឹត្តិការណ៍ EIGRP សំខាន់ៗ។

debug eigrp summary: ផ្តល់សេចក្តីសង្ខេបនៃសកម្មភាព EIGRP ។

show ip eigrp traffic: បង្ហាញស្ថិតិលើកញ្ចប់ EIGRP ដែលបានផ្ញើ និងទទួល។

តើ EIGRP support aggregation និង variable-length subnet masks? បាទ EIGRP គាំទ្រយ៉ាងពេញលេញទាំង aggregation (route summarization) និង Variable Length Subnet Masks (VLSM) ។

Aggregation (Summarization): EIGRP អនុញ្ញាតឱ្យ manual route summarization នៅលើ interface boundaries ដោយប្រើ command ip summary-address eigrp ។ នេះជួយកាត់បន្ថយទំហំ routing tables និងកំណត់ query floods ។

VLSM: EIGRP គឺជា classless routing protocol ដែលមានន័យថាវាបញ្ចូលព័ត៌មាន subnet mask នៅក្នុង routing updates របស់វា។ នេះអនុញ្ញាតឱ្យប្រើ VLSM ដែលអាចឱ្យការប្រើប្រាស់ IP address space ប្រកបដោយប្រសិទ្ធភាពដោយអនុញ្ញាតឱ្យប្រវែង subnet mask ផ្សេងៗគ្នានៅក្នុង major network តែមួយ។

តើខ្ញុំអាច configure ច្រើនជាងមួយ ប្រព័ន្ធស្វយ័ត EIGRP នៅលើ router តែមួយបានទេ? បាទ អ្នកអាចកំណត់រចនាសម្ព័ន្ធ autonomous system EIGRP ច្រើនជាងមួយ (AS) នៅលើ Cisco router តែមួយ។ នេះត្រូវបានសម្រេចដោយដំណើរការ EIGRP processes ជាច្រើន ដែលនីមួយៗមាន AS number ផ្សេងគ្នា។ នេះអាចមានប្រយោជន៍ក្នុងសេណារីយ៉ូដែល router ត្រូវការចូលរួមក្នុង EIGRP domains ផ្សេងៗគ្នា ឧទាហរណ៍ ក្នុងអំឡុងពេល network mergers ឬនៅពេល interconnecting បណ្តាញ EIGRP ដាច់ដោយឡែក។

តើអ្វីជាភាពខុសគ្នាសំខាន់ៗរវាង IPv4 និង IPv6?

|  |  |  |
| --- | --- | --- |
| លក្ខណៈពិសេស | IPv4 | IPv6 |
| ប្រវែងអាសយដ្ឋាន | 32-bit | 128-bit |
| ទម្រង់អាសយដ្ឋាន | Dotted decimal (ឧទាហរណ៍ 192.168.1.1) | Hexadecimal with colons (ឧទាហរណ៍ 2001:db8::1) |
| ទំហំអាសយដ្ឋាន | មានកំណត់ (~4.3 ពាន់លានអាសយដ្ឋានពិសេស) | ធំសម្បើម (2128 អាសយដ្ឋានពិសេស) |
| Header | ធំជាង ស្មុគស្មាញជាង | សាមញ្ញជាង ទំហំថេរ ប្រសិទ្ធភាពជាង |
| Checksum | មាននៅក្នុង header | មិនមាននៅក្នុង header |
| Fragmentation | គ្រប់គ្រងដោយ routers | គ្រប់គ្រងតែដោយ sending host ប៉ុណ្ណោះ |
| Broadcast | គាំទ្រ broadcast addresses | ត្រូវបានជំនួសដោយ multicast និង anycast |
| IPSec | ស្រេចចិត្ត | បង្កប់ស្រាប់ (native) |
| Mobility | Mobile IP បន្ថែមនៅពេលក្រោយ | ការគាំទ្រដោយធម្មជាតិប្រសើរជាងមុន |
| ការកំណត់រចនាសម្ព័ន្ធ | ដោយដៃ, DHCP | ដោយដៃ, DHCPv6, SLAAC |
| DNS Records | A records | AAAA records |

Export to Sheets

ពន្យល់ពីគោលបំណងនៃ subnetting ក្នុងបណ្តាញ។ គោលបំណងនៃ subnetting នៅក្នុងបណ្តាញគឺដើម្បីបែងចែកបណ្តាញធំមួយទៅជា subnets តូចៗ និងងាយស្រួលគ្រប់គ្រង។ នេះផ្តល់អត្ថប្រយោជន៍ជាច្រើន:

ប្រសិទ្ធភាពប្រសើរឡើង: កាត់បន្ថយទំហំនៃ broadcast domains ដែលនាំឱ្យចរាចរណ៍ broadcast តិច និងដំណើរការបណ្តាញប្រសើរឡើង។

សុវត្ថិភាពប្រសើរឡើង: អនុញ្ញាតឱ្យញែកផ្នែកបណ្តាញ ដែលការពារការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាតទៅកាន់តំបន់រសើប និងទប់ស្កាត់ការបំពានសុវត្ថិភាព។

ការគ្រប់គ្រងបណ្តាញកាន់តែប្រសើរ: ធ្វើឱ្យវាកាន់តែងាយស្រួលក្នុងការគ្រប់គ្រង និងដោះស្រាយបញ្ហាបណ្តាញដោយកំណត់បញ្ហាទៅ subnets ជាក់លាក់។

ការប្រើប្រាស់អាសយដ្ឋាន IP ប្រសើរបំផុត: អនុញ្ញាតឱ្យការបែងចែកអាសយដ្ឋាន IP កាន់តែមានប្រសិទ្ធភាព ជាពិសេសជាមួយ Variable Length Subnet Masking (VLSM) ដោយប្រើតែចំនួន hosts ដែលចាំបាច់ក្នុងមួយ subnet ។

ការរចនាជាឋានានុក្រម: អនុញ្ញាតឱ្យមានការរចនាបណ្តាញដែលមានរចនាសម្ព័ន្ធ និងឋានានុក្រមជាងមុន ដែលមានសារៈសំខាន់សម្រាប់បណ្តាញទ្រង់ទ្រាយធំ។

តើ ARP (Address Resolution Protocol) ដំណើរការយ៉ាងដូចម្តេចនៅក្នុងបរិយាកាសអន្តរបណ្តាញ? ARP (Address Resolution Protocol) គឺជា protocol Layer 2 ដែលត្រូវបានប្រើដើម្បីបំប្លែងអាសយដ្ឋាន IPv4 ទៅជាអាសយដ្ឋាន MAC (Layer 2 physical address) នៅក្នុង local network segment ។ វាដំណើរការដូចខាងក្រោម:

ARP Request: នៅពេលដែលឧបករណ៍មួយ (ឧទាហរណ៍ PC1) ចង់ផ្ញើទិន្នន័យទៅឧបករណ៍មួយទៀត (ឧទាហរណ៍ PC2) នៅលើ local network segment ដូចគ្នា ហើយវាគ្រាន់តែដឹងអាសយដ្ឋាន IP របស់ PC2 ប៉ុន្តែមិនមែនអាសយដ្ឋាន MAC របស់វាទេ PC1 ផ្ញើ ARP request ។ request នេះគឺជា broadcast message (ផ្ញើទៅឧបករណ៍ទាំងអស់នៅលើ segment) ដែលមានអាសយដ្ឋាន IP របស់ PC2 និងអាសយដ្ឋាន MAC និង IP របស់ PC1 ផ្ទាល់។

ARP Reply: ឧបករណ៍ទាំងអស់នៅលើ segment ទទួលបាន ARP request ។ មានតែឧបករណ៍ដែលជាម្ចាស់អាសយដ្ឋាន IP ដែលបានស្នើសុំ (PC2 ក្នុងករណីនេះ) ឆ្លើយតបជាមួយនឹង ARP reply ។ ARP reply មានអាសយដ្ឋាន MAC របស់ PC2 ហើយត្រូវបានផ្ញើជា unicast message ដោយផ្ទាល់ទៅ PC1 ។

ARP Cache: PC1 ទទួលបាន ARP reply ហើយរក្សាទុកការ mapping អាសយដ្ឋាន IP-to-MAC នៅក្នុង ARP cache របស់វាសម្រាប់ការប្រើប្រាស់នាពេលអនាគត។ នេះជៀសវាងការផ្ញើ ARP request សម្រាប់រាល់កញ្ចប់។

Inter-Network Communication: ប្រសិនបើ destination IP address ស្ថិតនៅលើបណ្តាញផ្សេងគ្នា ឧបករណ៍ដែលផ្ញើនឹងបញ្ជូនកញ្ចប់ទៅ default gateway របស់វា (router) ។ router បន្ទាប់មកអនុវត្តដំណើរការ ARP ផ្ទាល់ខ្លួនរបស់វាដើម្បីកំណត់អាសយដ្ឋាន MAC របស់ next-hop router ឬ destination device នៅលើ network segment បន្ទាប់។

ពន្យល់ពីរបៀបដែលពិធីការនាំផ្លូវ OSPF (បើកផ្លូវខ្លីបំផុតដំបូង) ដំណើរការ។ OSPF គឺជា link-state routing protocol ដែលដំណើរការដោយ router នីមួយៗគណនាដោយឯករាជ្យនូវផ្លូវខ្លីបំផុតទៅកាន់ destinations ដែលស្គាល់ទាំងអស់។ នេះជារបៀបដែលវាដំណើរការជាទូទៅ:

Neighbor Discovery: OSPF routers ផ្ញើកញ្ចប់ Hello ចេញពី OSPF-enabled interfaces របស់ពួកវាដើម្បីរកឃើញ និងបង្កើតទំនាក់ទំនង neighbor ។

Adjacency Formation: នៅពេលដែលទំនាក់ទំនង neighbor ត្រូវបានបង្កើត (ស្ថានភាព 2-way) routers ផ្លាស់ប្តូរ Database Description (DBD) packets ដើម្បីចែករំលែកសេចក្តីសង្ខេបនៃ Link-State Databases (LSDBs) របស់ពួកវា។ ប្រសិនបើ router រកឃើញថាវាបាត់ LSAs ពី neighbor វានឹងផ្ញើ Link State Request (LSR) packets ដើម្បីស្នើសុំព័ត៌មានដែលបាត់។ neighbor បន្ទាប់មកផ្ញើ Link State Update (LSU) packets ដែលមាន LSAs ដែលបានស្នើសុំ។

LSDB Synchronization: តាមរយៈការផ្លាស់ប្តូរនេះ routers ទាំងអស់នៅក្នុង OSPF area បង្កើត Link-State Database (LSDB) ដែលដូចគ្នា ដែលជាផែនទី topological ពេញលេញនៃ area នោះ។

SPF Algorithm (Dijkstra): Router នីមួយៗបន្ទាប់មកប្រើ algorithm Shortest Path First (SPF) របស់ Dijkstra ដើម្បីគណនា shortest path tree ទៅកាន់ destinations ដែលស្គាល់ទាំងអស់ ដោយខ្លួនវាជា root ។ "cost" នៃ link (interface) ត្រូវបានប្រើជា metric សម្រាប់ការគណនានេះ (default គឺផ្អែកលើ bandwidth) ។

Routing Table Population: ផ្លូវល្អបំផុតដែលកំណត់ដោយ SPF algorithm ត្រូវបានដំឡើងទៅក្នុង IP routing table របស់ router ។

Updates: នៅពេលដែលការផ្លាស់ប្តូរកើតឡើងនៅក្នុង network topology (ឧទាហរណ៍ link មួយ down, link ថ្មីមួយ up) router ដែលរងផលប៉ះពាល់បង្កើត LSA ថ្មី flooding វាទៅក្នុង area របស់វា ហើយ routers ផ្សេងទៀត update LSDBs របស់ពួកវា និងដំណើរការ SPF algorithm ឡើងវិញដើម្បី converge យ៉ាងឆាប់រហ័ស។

តើ BGP (Border Gateway Protocol) គឺជាអ្វី ហើយហេតុអ្វីបានជាវាសំខាន់នៅក្នុងអ៊ីនធឺណិត?

BGP (Border Gateway Protocol): BGP គឺជា exterior gateway protocol (EGP) ស្តង់ដារដែលត្រូវបានប្រើសម្រាប់ការ routing រវាង autonomous systems (AS) នៅលើអ៊ីនធឺណិត។ មិនដូច interior gateway protocols (IGPs) ដូចជា OSPF ឬ EIGRP ដែល route នៅក្នុង AS ទេ BGP route រវាង ASes ផ្សេងៗគ្នា។ វាគឺជា path-vector routing protocol ។

សារៈសំខាន់នៅក្នុងអ៊ីនធឺណិត:

ភ្ជាប់ Autonomous Systems: BGP មានសារៈសំខាន់ជាមូលដ្ឋានចំពោះរចនាសម្ព័ន្ធរបស់អ៊ីនធឺណិត ព្រោះវាអាចឱ្យការផ្លាស់ប្តូរព័ត៌មាន routing រវាងបណ្តាញឯករាជ្យរាប់ម៉ឺន (ASes) ដែលបង្កើតបានជាអ៊ីនធឺណិត។

Scalability: វាត្រូវបានរចនាឡើងដើម្បីគ្រប់គ្រងទំហំដ៏ធំនៃ routing table របស់អ៊ីនធឺណិត ដោយផ្ទុកផ្លូវរាប់រយរាប់ពាន់។

Policy-Based Routing: BGP អនុញ្ញាតឱ្យអ្នកគ្រប់គ្រងបណ្តាញអនុវត្ត policy routing ដ៏ស្មុគស្មាញដោយផ្អែកលើ attributes ផ្សេងៗ (ឧទាហរណ៍ AS Path, Local Preference, MED) ដើម្បីគ្រប់គ្រងរបៀបដែលចរាចរណ៍ចូល និងចេញពី AS របស់ពួកគេ។ នេះមានសារៈសំខាន់សម្រាប់ការ engineering ចរាចរណ៍ និងការសម្រេចបាននូវគោលបំណងអាជីវកម្ម។

ស្ថេរភាព និងការគ្រប់គ្រង: BGP ត្រូវបានរចនាឡើងសម្រាប់ស្ថេរភាព និងផ្តល់យន្តការដើម្បីការពារ routing loops និងធានាភាពសុចរិតនៃព័ត៌មាន routing ឆ្លងកាត់អ៊ីនធឺណិត។

ចូរពិពណ៌នាអំពី Verification Commands ក្នុង BGP routing protocol មានអ្វីខ្លះ។ ដើម្បីពិនិត្យមើលប្រតិបត្តិការ BGP អ្នកអាចប្រើ commands show មួយចំនួន:

show ip bgp summary: ផ្តល់ទិដ្ឋភាពសង្ខេបអំពីទំនាក់ទំនង neighbor BGP រួមទាំងស្ថានភាព សារដែលបានផ្លាស់ប្តូរ និងចំនួន prefix ។

show ip bgp: បង្ហាញខ្លឹមសារនៃ BGP routing table រួមទាំង prefixes ព័ត៌មាន next-hop និង BGP attributes ។

show ip bgp neighbors: បង្ហាញព័ត៌មានលម្អិតអំពី BGP neighbors រួមទាំងការកំណត់រចនាសម្ព័ន្ធ សមត្ថភាព និងស្ថិតិ session ។

show ip bgp [network-address]: បង្ហាញព័ត៌មាន BGP សម្រាប់បណ្តាញជាក់លាក់មួយ។

show ip bgp regexp [regular-expression]: ច្រោះ BGP routes ដោយប្រើ regular expression ។

show ip bgp longer-prefixes [network-address]: បង្ហាញផ្លូវជាក់លាក់បន្ថែមទៀតសម្រាប់បណ្តាញដែលបានផ្តល់ឱ្យ។

show ip protocols: រួមបញ្ចូលព័ត៌មានអំពី BGP routing protocol ។

តើ NAT ជួយក្នុងការរក្សាទុក IP Address យ៉ាងដូចម្តេច? NAT (Network Address Translation) ជួយក្នុងការរក្សាទុកអាសយដ្ឋាន IP ដោយអនុញ្ញាតឱ្យឧបករណ៍ជាច្រើននៅក្នុង private network ចែករំលែកអាសយដ្ឋាន IP សាធារណៈមួយ ឬមួយចំនួននៅពេលចូលប្រើអ៊ីនធឺណិត។

Many-to-One Mapping: ជាធម្មតា private network ទាំងមូលអាចទំនាក់ទំនងជាមួយពិភពខាងក្រៅដោយប្រើអាសយដ្ឋាន IP សាធារណៈតែមួយ ឬមួយចំនួនតូចប៉ុណ្ណោះ។ នេះមានន័យថា ជំនួសឱ្យឧបករណ៍ខាងក្នុងនីមួយៗត្រូវការអាសយដ្ឋាន IP សាធារណៈពិសេសរៀងៗខ្លួន ពួកវាទាំងអស់ប្រើ translated public IP ។

Private Address Space: NAT ប្រើប្រាស់ការប្រើប្រាស់ private IP address ranges (ឧទាហរណ៍ 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) ដែលមិនអាច route បាននៅលើអ៊ីនធឺណិត។ ឧបករណ៍នៅក្នុង private network ប្រើអាសយដ្ឋានទាំងនេះ ហើយ NAT router បំប្លែងពួកវាទៅជាអាសយដ្ឋានសាធារណៈដែលអាច route បានជាសកល លុះត្រាតែការទំនាក់ទំនងត្រូវបានផ្តួចផ្តើមទៅកាន់អ៊ីនធឺណិត។

ការអភិរក្ស: នេះជួយសន្សំសំចៃទំហំអាសយដ្ឋានសាធារណៈ IPv4 ដែលមានកំណត់យ៉ាងសំខាន់ ព្រោះអង្គការនានាគ្រាន់តែត្រូវទទួលបានអាសយដ្ឋាន IP សាធារណៈពី ISP របស់ពួកគេពីរបីប៉ុណ្ណោះ ជំនួសឱ្យមួយសម្រាប់ឧបករណ៍នីមួយៗ។

ពិពណ៌នាអំពីដំណើរការរបស់ DHCP (Dynamic Host Configuration Protocol)។ DHCP (Dynamic Host Configuration Protocol) គឺជា protocol បណ្តាញដែលអនុញ្ញាតឱ្យ server មួយកំណត់អាសយដ្ឋាន IP និង parameters ទំនាក់ទំនងផ្សេងទៀត (ដូចជា subnet mask, default gateway, DNS servers) ដោយស្វ័យប្រវត្តិទៅឧបករណ៍ដែលបានតភ្ជាប់ទៅបណ្តាញ។ ដំណើរការនេះជាធម្មតារួមមានបួនជំហានសំខាន់ៗ ដែលត្រូវបានគេចងចាំថាជា DORA (Discover, Offer, Request, Acknowledge):

DHCP Discover: នៅពេលដែលឧបករណ៍ client (ឧទាហរណ៍ កុំព្យូទ័រ) ដំណើរការ ឬភ្ជាប់ទៅបណ្តាញ វា broadcast សារ DHCP Discover (ទៅ destination IP 255.255.255.255 និង MAC address FF:FF:FF:FF:FF:FF) ដើម្បីស្វែងរក DHCP servers ដែលមាន។

DHCP Offer: DHCP server ណាមួយដែលទទួលបានសារ Discover ហើយមានអាសយដ្ឋាន IP ដែលមាន នឹង broadcast សារ DHCP Offer ។ សារនេះរួមបញ្ចូលអាសយដ្ឋាន IP ដែលបានស្នើឡើងសម្រាប់ client, subnet mask, default gateway, អាសយដ្ឋាន DNS server, និងរយៈពេលជួល។

DHCP Request: client ទទួលបានសារ DHCP Offer មួយឬច្រើន។ វាជ្រើសរើស offer មួយ (ជាធម្មតាជាលើកដំបូងដែលវាទទួលបាន) ហើយ broadcast សារ DHCP Request ដើម្បីទទួលយកជាផ្លូវការនូវអាសយដ្ឋាន IP និង parameters ដែលបានផ្តល់ជូន។ ការ broadcast នេះធានាថា DHCP servers ផ្សេងទៀតដឹងថា offers របស់ពួកវាមិនត្រូវបានទទួលយកទេ។

DHCP Acknowledge (ACK): DHCP server ដែលបានជ្រើសរើសទទួលបានសារ Request ហើយផ្ញើសារ DHCP ACK (Acknowledgment) ទៅ client ។ សារនេះបញ្ជាក់ការជួលអាសយដ្ឋាន IP និង parameters ការកំណត់រចនាសម្ព័ន្ធទាំងអស់។ client បន្ទាប់មកកំណត់រចនាសម្ព័ន្ធ network interface របស់វាជាមួយនឹងព័ត៌មានដែលបានទទួល ហើយអាចចាប់ផ្តើមទំនាក់ទំនងនៅលើបណ្តាញ។

ប្រៀបធៀប TCP និង UDP ក្នុងលក្ខខណ្ឌនៃភាពអាចជឿជាក់បាន និងករណីប្រើប្រាស់។ (បានគ្របដណ្តប់រួចហើយនៅក្នុងសំណួរទី 7) ។

តើអ្វីទៅការ configuration neighbor statement នៅក្នុង EIGRP? statement neighbor នៅក្នុង EIGRP ត្រូវបានប្រើសម្រាប់ការកំណត់រចនាសម្ព័ន្ធ EIGRP neighbors static ។ មិនដូច OSPF ឬ BGP ទេ EIGRP ជាធម្មតាប្រើ multicast Hellos (224.0.0.10) សម្រាប់ការរកឃើញ neighbor ដូច្នេះការកំណត់រចនាសម្ព័ន្ធ neighbors ដោយផ្ទាល់ជាធម្មតាមិនចាំបាច់នៅក្នុងបរិស្ថាន broadcast multi-access ទេ។ ទោះយ៉ាងណាក៏ដោយ command neighbor មានសារៈសំខាន់នៅក្នុងបណ្តាញ non-broadcast multi-access (NBMA) (ដូចជា Frame Relay, ATM, ឬពេលខ្លះ VPNs) ដែល multicast មិនត្រូវបានគាំទ្រ ឬមិនចង់បាន។

Syntax:

neighbor [ip-address] [interface-type interface-number]

ip-address: អាសយដ្ឋាន IP របស់ EIGRP neighbor ។

interface-type interface-number: interface ក្នុងស្រុកដែល neighbor អាចទៅដល់បាន។

ការប្រើប្រាស់: នៅពេលអ្នកកំណត់រចនាសម្ព័ន្ធ statement neighbor router នឹងផ្ញើ unicast EIGRP Hellos ទៅកាន់អាសយដ្ឋាន IP ជាក់លាក់នោះ ជំនួសឱ្យការពឹងផ្អែកលើ multicast discovery ។ នេះបង្ខំឱ្យមានទំនាក់ទំនង neighbor ជាមួយ router ដែលបានបញ្ជាក់។

តើពាក្យ serno មានន័យអ្វី នៅខាងចុងនៃ EIGRP topology ដោយសសេរ command បង្ហាញ ip eigrp topology? នៅពេលដែលអ្នកឃើញ "Serno" (ឬ "sequence number") នៅចុងបញ្ចប់នៃ EIGRP topology entry (ឧទាហរណ៍ show ip eigrp topology) វាសំដៅទៅលើ sequence number នៃ update packet ដែលបានផ្ទុកព័ត៌មានសម្រាប់ផ្លូវជាក់លាក់នោះ។ EIGRP ប្រើ sequence numbers សម្រាប់ការ reliable transport (RTP) នៃ update packets ។ រាល់ EIGRP update ដែលបានផ្ញើមាន sequence number ។ នៅពេលដែល router ទទួលបាន update វា acknowledges វាជាមួយនឹង sequence number ដែលត្រូវគ្នា។ "Serno" នៅក្នុង topology table បង្ហាញពី sequence number នៃ update ពី successor (ឬ feasible successor) ដែលបានផ្សាយផ្លូវជាក់លាក់នោះ។ វាគឺជាជំនួយក្នុងការដោះស្រាយបញ្ហាដើម្បីតាមដានភាពទាន់សម័យ និងប្រភពនៃព័ត៌មាន routing ។

តើអ្វីទៅ VPN IPSEC Tunnel? VPN (Virtual Private Network) IPSec Tunnel គឺជាការតភ្ជាប់ដែលមានសុវត្ថិភាព អ៊ិនគ្រីប (ជា "tunnel") ដែលត្រូវបានបង្កើតឡើងនៅលើបណ្តាញដែលមិនមានសុវត្ថិភាព (ដូចជាអ៊ីនធឺណិត) ដើម្បីផ្តល់ការទំនាក់ទំនងឯកជនរវាង endpoints ពីរ ឬច្រើន។ IPSec (Internet Protocol Security) គឺជាសំណុំ protocols ដែលផ្តល់សុវត្ថិភាពសម្រាប់ការទំនាក់ទំនង IP ដោយការ authenticate និង encrypt រាល់កញ្ចប់ IP ។

VPN: បង្កើតបណ្តាញ "ឯកជន" ឡូជីខលមួយនៅលើហេដ្ឋារចនាសម្ព័ន្ធសាធារណៈ អនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ពីចម្ងាយ ឬសាខាអាចចូលប្រើបណ្តាញកណ្តាលប្រកបដោយសុវត្ថិភាព ដូចជាពួកវាត្រូវបានតភ្ជាប់ដោយផ្ទាល់។

IPSec: ផ្តល់សេវាកម្ម cryptographic (encryption, authentication, integrity) ដែលធានា VPN tunnel ។ វាដំណើរការនៅ network layer (Layer 3) ហើយអាច encrypt កញ្ចប់ IP ទាំងមូល (tunnel mode) ឬតែ payload (transport mode) ។

Tunnel: សំដៅទៅលើការ encapsulation នៃ original IP packets នៅក្នុង IP packets ថ្មី ដែលបន្ទាប់មកត្រូវបាន encrypted និងផ្ញើឆ្លងកាត់ public network ។ នៅចុងម្ខាងទៀត outer headers ត្រូវបានដកចេញ កញ្ចប់ត្រូវបាន decrypted ហើយ original packet ត្រូវបានបញ្ជូន។

គេអោយរូបដូចខាងក្រោម នៃការ configure VPN IPSEC (Page 5), ចូរបំពេញ... ខាងក្រោម

A-លើ router PP1

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 2

!

crypto isakmp key [YOUR\_PRESHARED\_KEY] address [TK1\_Public\_IP\_Address] // Pre-shared key for TK1

!

crypto isakmp identity [local-id | hostname] // Often omitted if using pre-shared key by IP

!

crypto ipsec transform-set TS\_PP1\_TK1 esp-aes 256 esp-sha-hmac // Define transform set

!

crypto map CMAP\_PP1 1 ipsec-isakmp

set peer [TK1\_Public\_IP\_Address]

set transform-set TS\_PP1\_TK1

match address 101 // Assuming access-list 101 defines interesting traffic

!

interface [Interface\_Facing\_ISP] // e.g., GigabitEthernet0/1

crypto map CMAP\_PP1

!

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 // Interesting traffic

B-លើ router TK1

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 2

!

crypto isakmp key [YOUR\_PRESHARED\_KEY] address [PP1\_Public\_IP\_Address] // Pre-shared key for PP1

!

crypto isakmp identity [local-id | hostname] // Often omitted if using pre-shared key by IP

!

crypto ipsec transform-set TS\_TK1\_PP1 esp-aes 256 esp-sha-hmac // Define transform set

!

crypto map CMAP\_TK1 1 ipsec-isakmp

set peer [PP1\_Public\_IP\_Address]

set transform-set TS\_TK1\_PP1

match address 101 // Assuming access-list 101 defines interesting traffic

!

interface [Interface\_Facing\_ISP] // e.g., GigabitEthernet0/1

crypto map CMAP\_TK1

!

access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 // Interesting traffic (reverse of PP1)

ចំណាំ: ជំនួស [YOUR\_PRESHARED\_KEY], [TK1\_Public\_IP\_Address], [PP1\_Public\_IP\_Address], និង [Interface\_Facing\_ISP] ដោយតម្លៃជាក់ស្តែងរបស់អ្នក។

តើធ្វើដូចម្តេចដើម្បី IPSec VPN ទិសដៅជាច្រើនបានភ្ជាប់ Cisco? IPSec VPN tunnels ជាច្រើនទៅកាន់ destinations ផ្សេងៗគ្នានៅលើ Cisco routers អាចត្រូវបានកំណត់រចនាសម្ព័ន្ធតាមវិធីជាច្រើន:

Multiple Crypto Maps: សម្រាប់ site-to-site VPNs អ្នកអាចកំណត់រចនាសម្ព័ន្ធ crypto map entries ជាច្រើន (ជាមួយនឹង sequence numbers ផ្សេងគ្នា) នៅក្រោម crypto map set តែមួយ។ entry នីមួយៗអាចចង្អុលទៅ peer ផ្សេងគ្នា និងកំណត់ traffic គួរឱ្យចាប់អារម្មណ៍ផ្សេងគ្នាសម្រាប់ tunnel នោះ។

crypto map MY\_MAP 10 ipsec-isakmp

set peer [Peer\_IP\_1]

match address 101

crypto map MY\_MAP 20 ipsec-isakmp

set peer [Peer\_IP\_2]

match address 102

interface [ISP\_Facing\_Interface]

crypto map MY\_MAP

DMVPN (Dynamic Multipoint VPN): សម្រាប់ spoke-to-spoke និង spoke-to-hub VPNs, DMVPN ប្រើ NHRP (Next Hop Resolution Protocol) និង mGRE (multipoint GRE) tunnels ដើម្បីបង្កើត dynamic VPN tunnels តាមតម្រូវការ ធ្វើឱ្យការកំណត់រចនាសម្ព័ន្ធសាមញ្ញយ៉ាងខ្លាំងសម្រាប់ many-to-many scenarios ។

FlexVPN: ជាដំណោះស្រាយ VPN ទំនើប និងបត់បែនជាងមុនដែលអាចរួមបញ្ចូលបច្ចេកវិទ្យា VPN ផ្សេងៗ រួមទាំង IKEv2 និងសម្រួលការដាក់ពង្រាយ VPN ដ៏ស្មុគស្មាញ។

VTI (Virtual Tunnel Interface): VTI-based VPNs ផ្តល់ routable interface សម្រាប់ tunnel អនុញ្ញាតឱ្យ protocol routing ដំណើរការដោយផ្ទាល់លើ VPN tunnel សម្រួល routing និងការគ្រប់គ្រង។

ចូរពិពណ៌នាអំពីប្រភេទនៃ VPN Tunnels នៅលើ Cisco Routers។ Cisco routers គាំទ្រប្រភេទ VPN tunnels ផ្សេងៗគ្នា ដែលត្រូវបានបែងចែកជាទូទៅតាមបច្ចេកវិទ្យាមូលដ្ឋាន និងគោលបំណងរបស់ពួកវា:

IPSec VPNs: ប្រភេទទូទៅបំផុតសម្រាប់ secure site-to-site និង remote access VPNs ។ ពួកវាប្រើ IPSec សម្រាប់ការ encryption និង authentication ។

Site-to-Site IPSec VPN: ភ្ជាប់ទីតាំងថេរពីរ ឬច្រើន (ឧទាហរណ៍ សាខាទៅកាន់ទីស្នាក់ការកណ្តាល) លើអ៊ីនធឺណិត។

Remote Access IPSec VPN: អនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ម្នាក់ៗ (ឧទាហរណ៍ teleworkers) ភ្ជាប់ដោយសុវត្ថិភាពទៅ corporate network ពីទីតាំងដាច់ស្រយាល។

SSL VPNs (WebVPN/AnyConnect): ផ្តល់ secure remote access ដោយប្រើ SSL/TLS ជាធម្មតាសម្រាប់ web-based applications ឬ full network access តាមរយៈ client ។ ពួកវាគឺ clientless ឬប្រើ client ស្រាល។

GRE (Generic Routing Encapsulation) Tunnels: ផ្តល់វិធីមួយដើម្បី encapsulate protocols network layer យ៉ាងទូលំទូលាយនៅក្នុង IP tunnels ។ GRE ខ្លួនវាផ្ទាល់មិនផ្តល់ encryption ទេ ប៉ុន្តែត្រូវបានរួមបញ្ចូលជាញឹកញាប់ជាមួយ IPSec (GRE over IPSec) សម្រាប់ការ transport ប្រកបដោយសុវត្ថិភាព។

DMVPN (Dynamic Multipoint VPN): រួមបញ្ចូល mGRE, IPSec, និង NHRP ដើម្បីបង្កើតដំណោះស្រាយ VPN ដែលអាចពង្រីកបាន និង dynamic សម្រាប់ការតភ្ជាប់ hub-and-spoke និង spoke-to-spoke ។

VTI (Virtual Tunnel Interface) Based VPNs: ប្រើ virtual interfaces ជា tunnel endpoints អនុញ្ញាតឱ្យ protocol routing ដំណើរការដោយផ្ទាល់លើ VPN tunnel សម្រួល routing និងការគ្រប់គ្រង។

FlexVPN: ជាក្របខ័ណ្ឌបង្រួបបង្រួមដែលគាំទ្រ VPN deployments ផ្សេងៗ រួមទាំង IKEv2 និង mGRE ដែលផ្តល់ភាពបត់បែន និង scalability ។

តើទៅជាប្រភេទនៃ Address មានដូចជា Inside Local, Inside Global, Outside Global, និង Outside Local NAT ។ NAT ប្រើអាសយដ្ឋានបួនប្រភេទដើម្បីសម្រួលការបំប្លែង:

Inside Local Address: អាសយដ្ឋាន IP របស់ឧបករណ៍នៅលើ inside network (private network របស់អ្នក) ដូចដែលបានឃើញពីឧបករណ៍ផ្សេងទៀតនៅលើ inside network ។ ទាំងនេះជាធម្មតាជា private IP addresses (ឧទាហរណ៍ 192.168.1.10) ។

Inside Global Address: អាសយដ្ឋាន IP របស់ឧបករណ៍នៅលើ inside network ដូចដែលបានឃើញពី outside network (អ៊ីនធឺណិត) ។ នេះគឺជា public, globally routable IP address ដែលត្រូវបានកំណត់ដោយឧបករណ៍ NAT ។

Outside Local Address: អាសយដ្ឋាន IP របស់ឧបករណ៍នៅលើ outside network (ឧទាហរណ៍ web server នៅលើអ៊ីនធឺណិត) ដូចដែលបានឃើញពី inside network ។ នេះជាញឹកញាប់គឺជា public IP address ពិតប្រាកដរបស់ outside device ប៉ុន្តែវាក៏អាចជា translated address ប្រសិនបើ outside network ក៏កំពុងប្រើ NAT ដែរ។

Outside Global Address: អាសយដ្ឋាន IP របស់ឧបករណ៍នៅលើ outside network ដូចដែលបានឃើញពី outside network ។ នេះគឺជា globally routable IP address របស់ outside device ។ សម្រាប់ឧបករណ៍នៅលើអ៊ីនធឺណិត outside local និង outside global addresses ជាធម្មតាដូចគ្នា។

លំហាត់ ចូរសរសេរ command configure router ខាងក្រោម៖ នេះតម្រូវឱ្យកំណត់រចនាសម្ព័ន្ធ routing protocols និង/ឬ static routes ដើម្បីធានាថាបណ្តាញទាំងអស់ (NET 1, NET 2, NET 3, NET 4) អាចទៅដល់គ្នាទៅវិញទៅមក។ នេះជាការកំណត់រចនាសម្ព័ន្ធសម្រាប់វិធីសាស្ត្រ routing នីមួយៗដែលបានស្នើសុំ:

ការសន្មត់:

Interfaces ត្រូវបានកំណត់រចនាសម្ព័ន្ធតាមដ្យាក្រាមនៅលើទំព័រ 6 ។

Loopback interfaces (ប្រសិនបើប្រើសម្រាប់ router IDs) ត្រូវបានកំណត់រចនាសម្ព័ន្ធ (មិនបានបង្ហាញក្នុងឧទាហរណ៍ទេ ប៉ុន្តែជាការអនុវត្តល្អ) ។

1. ការកំណត់រចនាសម្ព័ន្ធ Static Routing:

Router1:

interface GigabitEthernet0/0

ip address 192.168.210.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 111.111.110.254 255.255.255.252

no shutdown

!

ip route 112.112.113.0 255.255.255.252 111.111.110.253 // Route to NET 3 via Router2

ip route 192.168.213.0 255.255.255.0 111.111.110.253 // Route to NET 4 via Router2

Router2:

interface Serial0/0/0

ip address 111.111.110.253 255.255.255.252

no shutdown

interface Serial0/0/1

ip address 112.112.113.254 255.255.255.252

no shutdown

!

ip route 192.168.210.0 255.255.255.0 111.111.110.254 // Route to NET 1 via Router1

ip route 192.168.213.0 255.255.255.0 112.112.113.253 // Route to NET 4 via Router3

Router3:

interface GigabitEthernet0/0

ip address 192.168.213.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 112.112.113.253 255.255.255.252

no shutdown

!

ip route 111.111.110.0 255.255.255.252 112.112.113.254 // Route to NET 2 via Router2

ip route 192.168.210.0 255.255.255.0 112.112.113.254 // Route to NET 1 via Router2

2. ការកំណត់រចនាសម្ព័ន្ធ Default Routing: ចំណាំ: Default routing ជាធម្មតាត្រូវបានប្រើនៅលើ edge routers (ឧទាហរណ៍ Router1 និង Router3) ដើម្បីចង្អុលទៅ central router (Router2) ឬអ៊ីនធឺណិត។

Router1:

ip route 0.0.0.0 0.0.0.0 111.111.110.253 // Default route to Router2

Router2:

// No default route needed here, as it's the central point.

// It should have static routes or dynamic routing to other networks.

// If it's the gateway to the internet, then a default route to ISP.

Router3:

ip route 0.0.0.0 0.0.0.0 112.112.113.254 // Default route to Router2

3. ការកំណត់រចនាសម្ព័ន្ធ EIGRP Routing:

Router1:

router eigrp 100

network 192.168.210.0 0.0.0.255 // NET 1

network 111.111.110.0 0.0.0.3 // NET 2

no auto-summary

Router2:

router eigrp 100

network 111.111.110.0 0.0.0.3 // NET 2

network 112.112.113.0 0.0.0.3 // NET 3

no auto-summary

Router3:

router eigrp 100

network 192.168.213.0 0.0.0.255 // NET 4

network 112.112.113.0 0.0.0.3 // NET 3

no auto-summary

4. ការកំណត់រចនាសម្ព័ន្ធ OSPF Routing:

Router1:

router ospf 1

network 192.168.210.0 0.0.0.255 area 0 // NET 1

network 111.111.110.0 0.0.0.3 area 0 // NET 2

Router2:

router ospf 1

network 111.111.110.0 0.0.0.3 area 0 // NET 2

network 112.112.113.0 0.0.0.3 area 0 // NET 3

Router3:

router ospf 1

network 192.168.213.0 0.0.0.255 area 0 // NET 4

network 112.112.113.0 0.0.0.3 area 0 // NET 3

ចំណាំ: សម្រាប់ភាពសាមញ្ញ routers ទាំងអស់ត្រូវបានដាក់នៅក្នុង Area 0 (backbone) ។ ក្នុងការរចនាធំជាងនេះ អ្នកអាចប្រើ areas ផ្សេងគ្នា។

5. ការកំណត់រចនាសម្ព័ន្ធ BGP Routing: ចំណាំ: BGP ជាធម្មតាត្រូវបានប្រើរវាង Autonomous Systems ។ សម្រាប់ការរៀបចំតូចនេះ ជាទូទៅវាលើសលប់ ប៉ុន្តែនេះគឺជាការកំណត់រចនាសម្ព័ន្ធគំនិត។ អ្នកនឹងត្រូវកំណត់ AS numbers ។

Router1 (AS 65001):

router bgp 65001

neighbor 111.111.110.253 remote-as 65002 // Peer with Router2

network 192.168.210.0 mask 255.255.255.0

network 111.111.110.0 mask 255.255.255.252

Router2 (AS 65002):

router bgp 65002

neighbor 111.111.110.254 remote-as 65001 // Peer with Router1

neighbor 112.112.113.253 remote-as 65003 // Peer with Router3

network 111.111.110.0 mask 255.255.255.252

network 112.112.113.0 mask 255.255.255.252

Router3 (AS 65003):

router bgp 65003

neighbor 112.112.113.254 remote-as 65002 // Peer with Router2

network 192.168.213.0 mask 255.255.255.0

network 112.112.113.0 mask 255.255.255.252

6. ការកំណត់រចនាសម្ព័ន្ធ RIP v2 Routing:

Router1:

router rip

version 2

network 192.168.210.0

network 111.111.110.0

no auto-summary

Router2:

router rip

version 2

network 111.111.110.0

network 112.112.113.0

no auto-summary

Router3:

router rip

version 2

network 192.168.213.0

network 112.112.113.0

no auto-summary