RIP Tutorial

February 3rd, 2011 Go to comments

In this tutorial we will learn about RIP routing protocol

Routing Information Protocol (RIP) is a distance-vector routing protocol which is based on Bellman-Ford algorithm. Routers using Distance Vector routing protocols do not posses the topological information about the network but instead rely on the neighbors information (so this method is known as routing by rumor). RIP sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count (the number of routers) to determine the best way to a remote network.

Note: RIP v1 is a classful routing protocol but RIP v2 is a classless routing protocol.

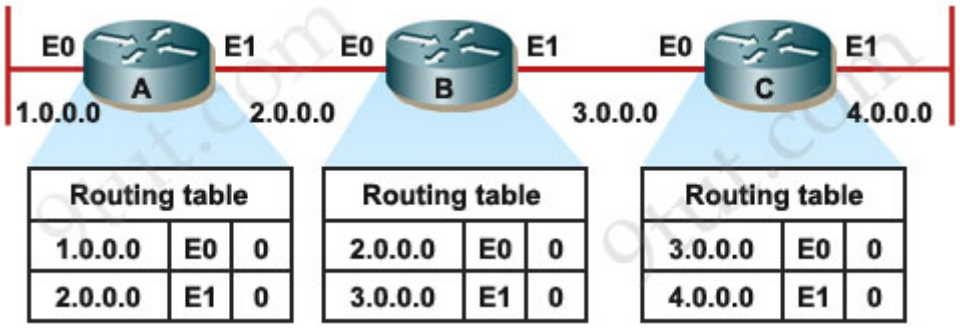
Classful routing protocols do not include the subnet mask with the network address in routing updates, which can cause problems with discontiguous subnets or networks that use Variable-Length Subnet Masking (VLSM). Fortunately, RIPv2 is a classless routing protocol so subnet masks are included in the routing updates, making RIPv2 more compatible with modern routing environments.

Distance vector protocols advertise routing information by sending messages, called routing updates, out the interfaces on a router.

RIP Operation

A big problem with distance vector routing protocol is routing loop. Let's take a look at how a routing loop occurs.

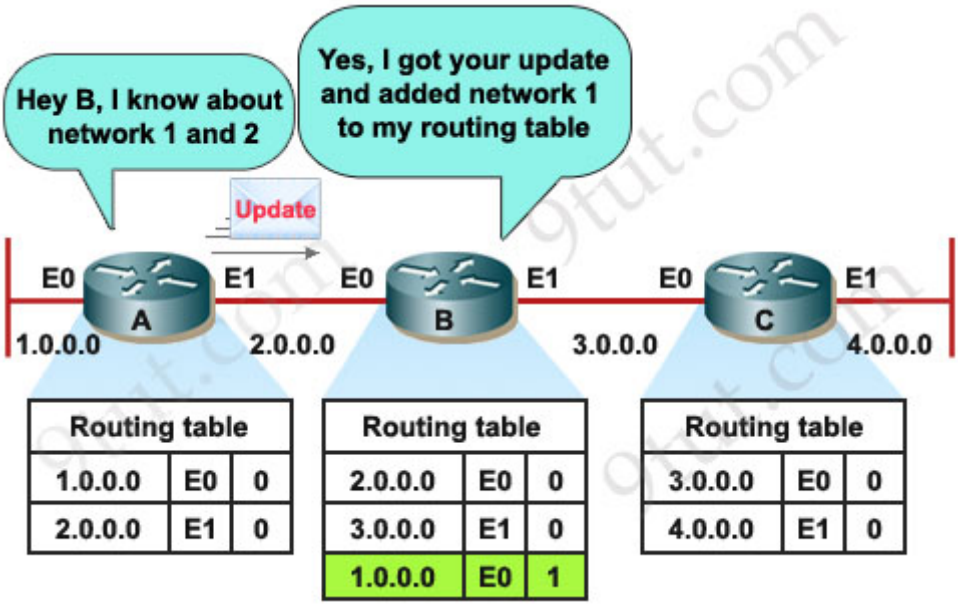
Here we have routers A, B and C. Notice that at the beginning (when a routing protocol is not turned on) there are only directly connected networks in the routing tables of these routers. For example, in the routing table of router A, **network 1.0.0.0** has already been known because it is directly connected through **interface E0** and the **metric** (of a directly connected network) is **0** (these 3 parameters are shown in the routing tables below).



Also B knows networks **2.0.0.0** & **3.0.0.0** with a **metric of 0**.
Also C knows networks **3.0.0.0** & **4.0.0.0** with a **metric of 0**.

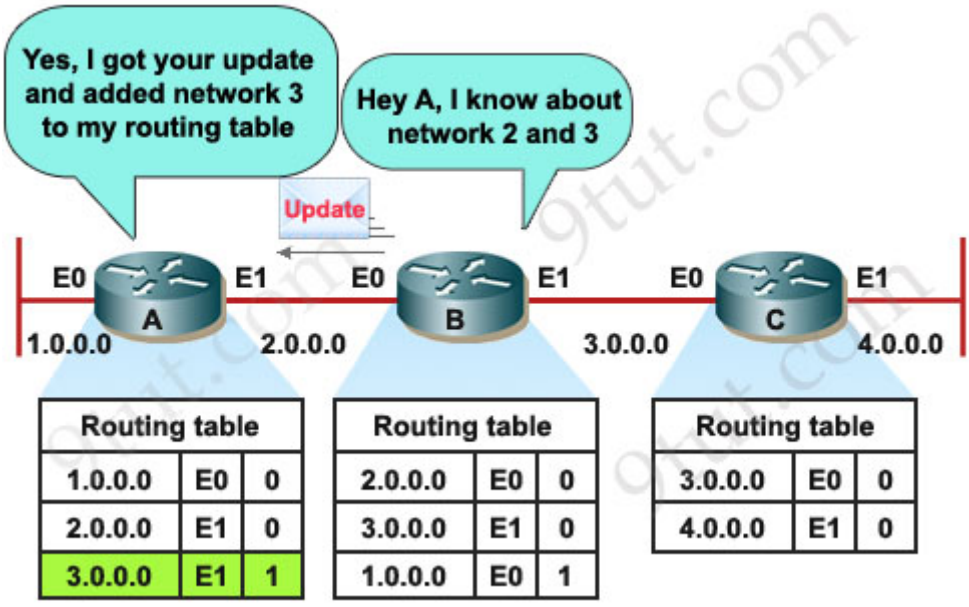
Now we turn on RIP on these routers (we will discuss the configuration later. In the rest of this article, we will call network 1.0.0.0 network 1, 2.0.0.0 network 2 and so on).

RIP sends update every 30 seconds so after 30 sec goes by, A sends a copy of its routing table to B, B already knew about network 2 but now B learns about network 1 as well. Notice the metric we have here for directly connected networks, since we're using RIP, we're using a metric of hop count. Remember a hop count (or a hop) is how many routers that these packets will have to go through to reach the destination. For example, from router A to network 1 & 2 (which are directly connected) it goes to 0 hop, router B has now learned about network 1 from A via E0 interface so the metric now will be 1 hop.

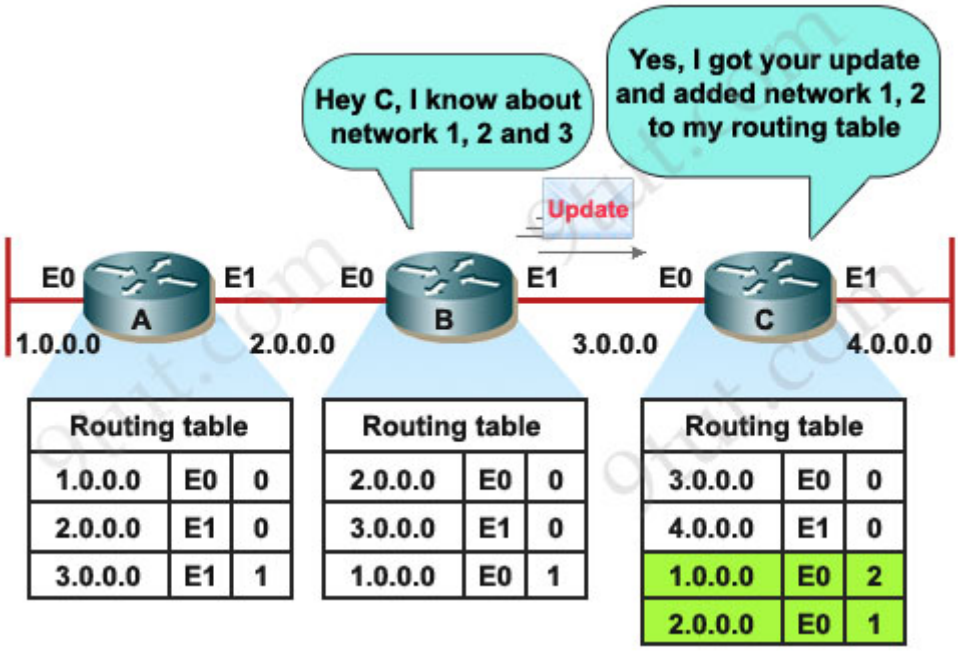


Each router receives a routing table from its direct neighbor. For example, Router B receives information from Router A about network 1 and 2. It then adds a distance vector metric (such as the number of hops), increasing the distance vector of these routes by 1.

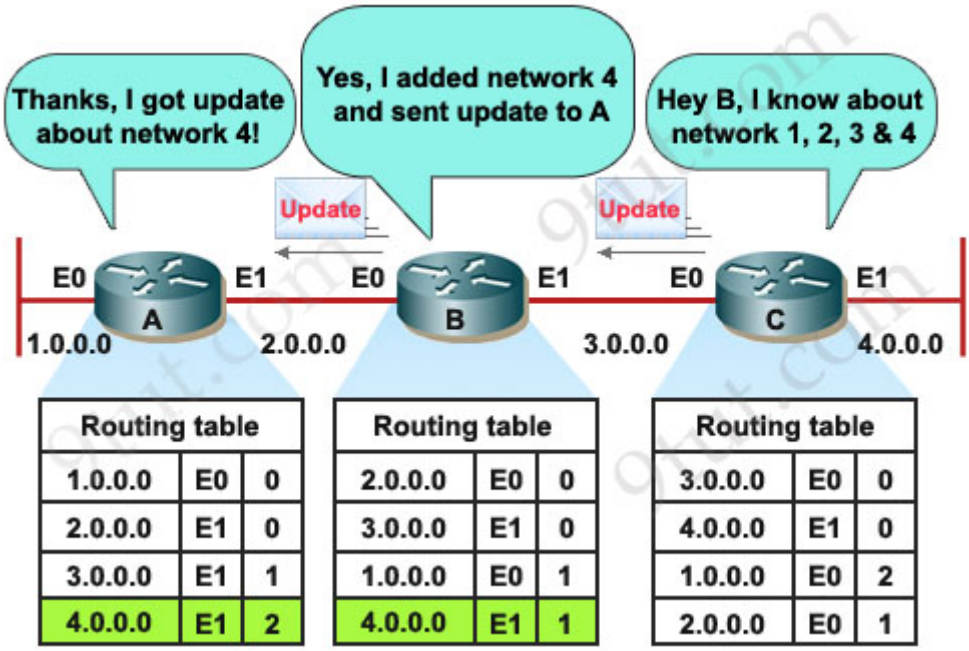
B also exchanges its routing table with A about network 2 and 3.



B then passes the routing table to its other neighbor, Router C.

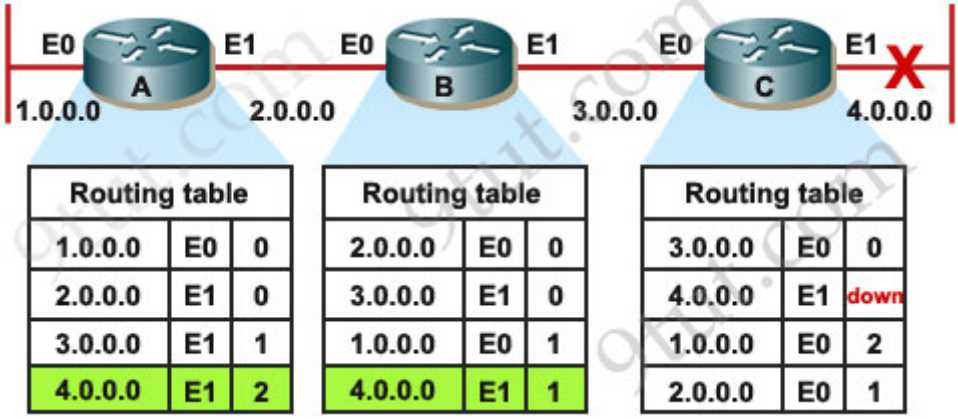


C also sends its update to B and B sends it to A.



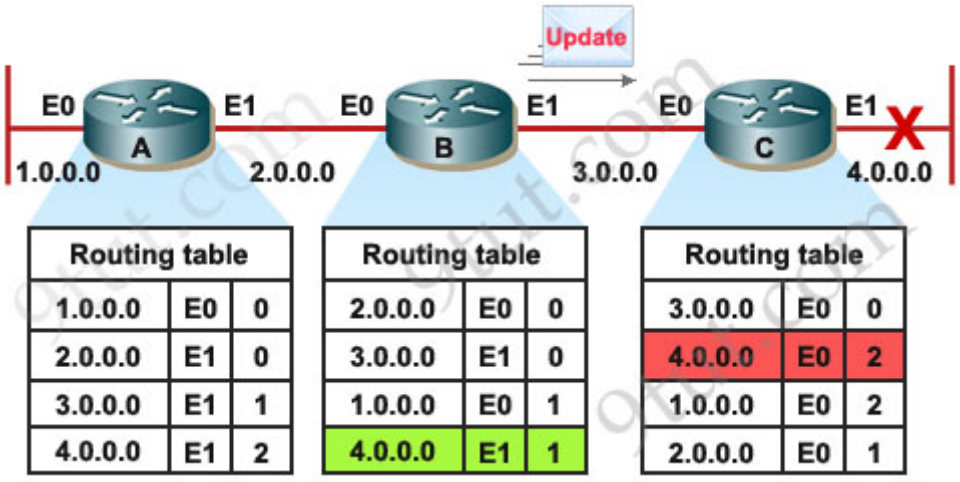
Now the network is converged.

Now let’s assume network 4 down suddenly.



When network 4 fails, Router C detects the failure and stops routing packets out its E1 interface. However, Routers A and B have not yet received notification of the failure. Router A still believes it can access 4.0.0.0 through Router B. The routing table of Router A still refects a path to network 10.4.0.0 with a distance of 2 and router B has a path with a distance of 1.

There will be no problem if C sends an update earlier than B and inform that network is currently down but if B sends its update first, C will see B has a path to network 4 with a metric of 1 so it updates its routing table, thinking that "if B can go to network 4 by 1 hop than I can go to network 4 by 2 hops" but of course this is totally wrong.

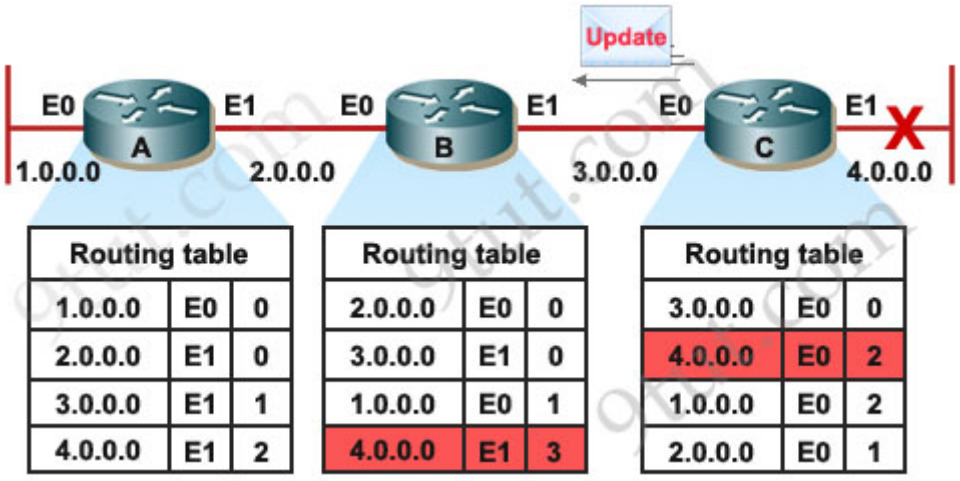


Routing table		
1.0.0.0	E0	0
2.0.0.0	E1	0
3.0.0.0	E1	1
4.0.0.0	E1	2

Routing table		
2.0.0.0	E0	0
3.0.0.0	E1	0
1.0.0.0	E0	1
4.0.0.0	E1	1

Routing table		
3.0.0.0	E0	0
4.0.0.0	E0	2
1.0.0.0	E0	2
2.0.0.0	E0	1

The problem does not stop here. In turn, C sends an update to B and informs it can access network 4 by 2 hops. B learns this and think "if C can access network 4 by 2 hops than I can access by 3 hops".



Routing table		
1.0.0.0	E0	0
2.0.0.0	E1	0
3.0.0.0	E1	1
4.0.0.0	E1	2

Routing table		
2.0.0.0	E0	0
3.0.0.0	E1	0
1.0.0.0	E0	1
4.0.0.0	E1	3

Routing table		
3.0.0.0	E0	0
4.0.0.0	E0	2
1.0.0.0	E0	2
2.0.0.0	E0	1

This same process occurs when B continually sends its update to C and the metric will increase to infinity so this phenomenon is called "counting to infinity".

Below lists some methods to prevent this phenomenon:

SPLIT HORIZON:
A router never sends information about a route back in same direction which is original information came, routers keep track of where the information about a route came from. Means when router A sends update to router B about any failure network, router B does not send any update for same network to router A in same direction.

ROUTE POISONING:
Router consider route advertised with an infinitive metric to have failed (metric=16) instead of marking it down. For example, when network 4 goes down, router C starts route poisoning by advertising the metric (hop count) of this network as 16, which indicates an unreachable network. When router B receives this advertising, it continue advertising this network with a metric of 16.

POISON REVERSE:

The poison reverse rule overwrites split horizon rule. For example, if router B receives a route poisoning of network 4 from router C then router B will send an update back to router C (which breaks the split horizon rule) with the same poisoned hop count of 16. This ensures all the routers in the domain receive the poisoned route update.

Notice that every router performs poison reverse when learning about a downed network. In the above example, router A also performs poison reverse when learning about the downed network from B.

HOLD DOWN TIMERS:

After hearing a route poisoning, router starts a hold-down timer for that route. If it gets an update with a better metric than the originally recorded metric within the hold-down timer period, the hold-down timer is removed and data can be sent to that network. Also within the hold-down timer, if an update is received from a different router than the one who performed route poisoning with an equal or poorer metric, that update is ignored. During the hold-down timer, the "downed" route appears as "possibly down" in the routing table.

For example, in the above example, when B receives a route poisoning update from C, it marks network 4 as "possibly down" in its routing table and starts the hold-down timer for network 4. In this period if it receives an update from C informing that the network 4 is recovered then B will accept that information, remove the hold-down timer and allow data to go to that network. But if B receives an update from A informing that it can reach network by 1 (or more) hop, that update will be ignored and the hold-down timer keeps counting.

Note: The default hold-down timer value = 180 second.

TRIGGERED UPDATE :
When any route failed in network ,do not wait for the next periodic update instead send an immediate update listing the poison route.

COUNTING TO INFINITY:
Maximum count 15 hops after it will not be reachable.

RIP Timers

RIP uses several timers to regulate its operation. These timers are described below:

Update timer: how often the router sends update. Default update timer is 30 seconds
Invalid timer (also called **Expire timer**): how much time must expire before a route becomes invalid since seeing a valid update; and place the route into holddown. Default invalid timer is 180 seconds
Holddown timer: When a route is expired, it enters "holddown", which means the router will not believe any new updates with a hop count equal to or higher (poorer) than the hop count recording in the routing table. Hold down is intended to assist in avoiding inaccurate routing by rumor information while the network converges. Default holddown timer is 180 seconds
Flush timer: how much time since the last valid update, until RIP deletes that route in its routing table. Default Flush timer is 240 seconds

Note: From the image above, you can see that when a route expires, in fact the Holddown timer only works in its first 60 seconds (not 180 seconds), then the route is removed from the routing table when the Flush timer is expired.

Configuring RIP

Router(config)#router rip	Enter router RIP configuration mode
Router(config-router)#network <*address*>	Identify networks that will participate in the router protocol. Notice that you identify networks, and not interfaces.

NOTE: You need to advertise only the classful network number, not a subnet:
Router(config-router)#network 172.16.0.0
not
Router(config-router)#network 172.16.10.0

If you advertise a subnet, you will not receive an error message, because the router will automatically convert the subnet to the classful network address.

To learn more about configuring RIP, please read my Configuring RIP GNS3 Lab tutorial

Key points:

+ RIP uses hop counts to calculate optimal routes (a hop is a router).
+ RIP routing is limited to 15 hops to any location (16 hops indicates the network is unreachable).
+ RIP uses the split horizon with poison reverse method to prevent the count-to-infinity problem.
+ RIP uses only classful routing, so it uses full address classes, not subnets.
+ RIP broadcasts updates to the entire network.
+ RIP can maintain up to six multiple paths to each network, but only if the cost is the same.
+ RIP supports load balancing over same-cost paths.
+ The update interval default is 30, the invalid timer default is 180, the holddown timer default is 180, and the flush timer default is 240.

Comments (2) Comments

1. Anwar
   May 18th, 2020

   this RIP topics was posted on February 3rd, 2011 as per the posted date.
   its been long time, 9 years , is there any changes or update came out by this time? or all are still same?
   or if the topics are updated with latest information, please update the date as well.

2. Anonymous

September 4th, 2021

Please update if any new feature added to RIP ?

Add a Comment

Name

Submit Comment

Subscribe to comments feed

CCNA – Hotspot CCNA – STP Questions

Premium Member Zone

Welcome Gurjeet singh!

- Welcome Premium Member
- CCNA – New Questions Part 5
- CCNA – New Questions Part 6
- CCNA – New Questions Part 7
- CCNA – New Questions Part 8
- CCNA – New Questions Part 9
- Composite Quizzes

- Logout

CCNA 200-301

- Basic Questions
- Topology Architecture Questions
- Cloud & Virtualization Questions
- CDP & LLDP Questions
- Switch Questions
- VLAN & Trunking Questions
- VLAN & Trunking Questions 2
- STP & VTP Questions
- EtherChannel Questions
- TCP & UDP Questions
- IP Address & Subnetting Questions
- IP Routing Questions
- IP Routing Questions 2
- OSPF Questions
- OSPF Questions 2
- EIGRP Questions
- NAT Questions
- NTP Questions

- Syslog Questions
- HSRP Questions
- Access-list Questions
- AAA Questions
- Security Questions
- Security Questions 2
- DAI Questions
- IPv6 Questions
- DNS Questions
- QoS Questions
- Port Security Questions
- Wireless Questions
- Wireless Questions 2
- SDN Questions
- DNA Center Questions
- Drag Drop Questions
- Drag Drop Questions 2
- Drag Drop Questions 3
- VPN Questions
- DHCP Questions
- Automation Questions
- Miscellaneous Questions
- CCNA FAQs & Tips
- Share your new CCNA Experience

CCNA Self-Study

- Practice CCNA GNS3 Labs
- CCNA Knowledge
- CCNA Lab Challenges
- Puppet Tutorial
- Chef Tutorial
- Ansible Tutorial
- JSON Tutorial
- Layer 2 Threats and Security Features
- AAA TACACS+ and RADIUS Tutorial
- STP Root Port Election Tutorial
- GRE Tunnel Tutorial
- Basic MPLS Tutorial
- TCP and UDP Tutorial
- Border Gateway Protocol BGP Tutorial
- Point to Point Protocol (PPP) Tutorial
- WAN Tutorial
- DHCP Tutorial
- Simple Network Management Protocol SNMP Tutorial
- Syslog Tutorial
- Gateway Load Balancing Protocol GLBP Tutorial
- EtherChannel Tutorial
- Hot Standby Router Protocol HSRP Tutorial
- InterVLAN Routing Tutorial
- Cisco Command Line Interface CLI
- Cisco Router Boot Sequence Tutorial
- OSI Model Tutorial
- Subnetting Tutorial – Subnetting Made Easy
- Frame Relay Tutorial
- Wireless Tutorial
- Virtual Local Area Network VLAN Tutorial

- VLAN Trunking Protocol VTP Tutorial
- IPv6 Tutorial
- Rapid Spanning Tree Protocol RSTP Tutorial
- Spanning Tree Protocol STP Tutorial
- Network Address Translation NAT Tutorial
- Access List Tutorial
- RIP Tutorial
- EIGRP Tutorial
- OSPF Tutorial

Network Resources

- Free Router Simulators
  - CCNA Website
  - ENCOR Website
  - ENSDWI Website
  - ENARSI Website
  - DevNet Website
  - CCIE R&S Website
  - Security Website
  - Wireless Website
  - Design Website
  - Data Center Website
  - Service Provider Website
  - Collaboration Website

Top