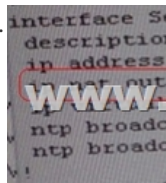


[17th/11/2017-NEWBraindump2go 300-135 Exam VCE and PDF 131Q for 100% Passing 300-135 Exam[52-62

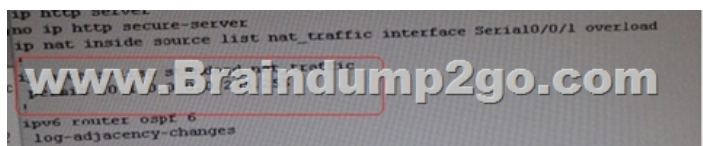
2017 November New 300-135 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 300-135 questions:1.|2017 New 300-135 Exam Dumps (PDF & VCE) 131Q&As Download:

<https://www.braindump2go.com/300-135.html>2.|2017 New 300-135 Exam Questions & Answers Download:

<https://drive.google.com/drive/folders/0B75b5xYLjSSNTFg2a1ZwLUwtNmM?usp=sharing>QUESTION 52The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolate the cause of this fault and answer the following questions. What is the solution to the fault condition?
A. Under the BGP process, enter the `bgp redistribute-internal` command.
B. Under the BGP process, `bgp confederation identifier 65001` command.
C. Deleted the current BGP process and reenter all of the command using 65002 as the AS number.
D. Under the BGP process, delete the `neighbor 209.56.200.226 remote-as 65002` command and enter the `neighbor 209.65.200.226 remote-as 65002` command.
Answer: D
Explanation: On R1 under router BGP change neighbor 209.56.200.226 remote-as 65002 statement to neighbor 209.65.200.226 remote-as 65002
Ticket 5 : NAT ACL Topology Overview (Actual Troubleshooting lab design is for below network design)- Client Should have IP 10.2.1.3- EIGRP 100 is running between switch DSW1 & DSW2- OSPF (Process ID 1) is running between R1, R2, R3, R4- Network of OSPF is redistributed in EIGRP- BGP 65001 is configured on R1 with Webserver cloud AS 65002- HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches. In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary. R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range. R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network. ASW1 and ASW2 are layer 2 switches. NTP is enabled on all devices with 209.65.200.226 serving as the master clock source. The client workstations receive their IP address and default gateway via R4's DHCP server. The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2. In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary. Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations. Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution. Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device.
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
Client is unable to ping IP 209.65.200.241
Solution: Steps need to follow as below:-
When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 Ipconfig ----- Client will be receiving IP address 10.2.1.3- IP 10.2.1.3 will be able to ping from R4, R3, R2, R1- Look for BGP Neighbourship
`Sh ip bgp summary` ----- State of BGP will be in established state & will be able to receive I prefix (209.65.200.241)- As per troubleshooting we are able to ping ip 10.2.1.3 from R1 & BGP is also receiving prefix of webserver & we are able to ping the same from R1. Further troubleshooting needs to be done on R1 on serial 0/0/1- Check for running config. i.e `sh run` for interface serial 0/0/1..



```
interface S
description
ip address
www
ntp broadc
ntp broadc
```



```
ip http server
no ip http secure-server
ip nat inside source list nat traffic interface Serial0/0/1 overload
www.Braindump2go.com
ip v6 router ospf 6
log-adjacency-changes
```

!From above snapshot we are able to see that IP needs to be PAT to serial 0/0/1 to reach web server IP (209.65.200.241). But in access-list of NAT IP allowed IP is 10.1.0.0/16 is allowed & need 10.2.0.0 /16 to- As per troubleshooting we are able to ping ip 10.2.1.3 from R1 & BGP is also receiving prefix of web server & we are able to ping the same from R1. Its should be checked further for running config of interface for stopping- Change required: On R1, In natting we need to add client IP address for reachability to server. QUESTION 53The implementations group has been using the test bed to do a `proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.Use the supported commands to isolated the cause of this fault and answer the following questions.On which device is the fault condition located?A. R1B. R2C. R3D. R4E. DSW1F. DSW2 G. ASW1Answer: AExplanation:On R1 we need to add the client IP address for reachability to server to the access list that is used to specify which hosts get NATed.QUESTION 54The implementations group has been using the test bed to do a `proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.Use the supported commands to isolated the cause of this fault and answer the following questions.The fault condition is related to which technology?A. BGPB. NTPC. IP NAT D. IPv4 OSPF RoutingE. IPv4 OSPF RedistributionF. IPv6 OSPF RoutingG. IPv4 layer 3 securityAnswer: CExplanation:On R1 we need to add the client IP address for reachability to server to the access list that is used to specify which hosts get NATed.QUESTION 55The implementations group has been using the test bed to do a `proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.Use the supported commands to isolated the cause of this fault and answer the following questions.What is the solution to the fault condition?A. Under the interface Serial0/0/0 configuration enter the ip nat inside command.B. Under the interface Serial0/0/0 configuration enter the ip nat outside command.C. Under the ip access-list standard nat_traffic configuration enter the permit 10.2.0.0 0.0.255.255 command.D. Under the ip access-list standard nat_traffic configuration enter the permit 209.65.200.0 0.0.255command.Answer: CExplanation:On R1 we need to add the client IP address for reachability to server to the access list that is used to specify which hosts get NATed.Ticket 6 : R1 ACLTopology Overview (Actual Troubleshooting lab design is for below network design)- Client Should have IP 10.2.1.3- EIGRP 100 is running between switch DSW1 & DSW2- OSPF (Process ID 1) is running between R1, R2, R3, R4- Network of OSPF is redistributed in EIGRP- BGP 65001 is configured on R1 with Webserver cloud AS 65002- HSRP is running between DSW1 & DSW2 SwitchesThe company has created the test bed shown in the layer 2 and layer 3 topology exhibits.This network consists of four routers, two layer 3 switches and two layer 2 switches.In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.ASW1 and ASW2 are layer 2 switches.NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.The client workstations receive their IP address and default gateway via R4's DHCP server.The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.Recently the implementation group has been using the test bed to do a `proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.Each ticket has 3 sub questions that need to be answered & topology remains same.Question-1 Fault is found on which device,Question-2 Fault condition is related to,Question-3 What exact problem is seen & what needs to be done for solutionClient is unable to ping IP 209.65.200.241...Solution:Steps need to follow as below:- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4- Ipconfig ----- Client will be receiving IP address 10.2.1.3- IP 10.2.1.3 will be able to ping from R4 , R3, R2, R1- Look for BGP Neighbourship- Sh ip bgp summary ----- State of BGP will be in active state. This means connectivity issue between serial- Check for running config. i.e sh run --- over here check for access-list configured on interface as BGP is down (No need to check for NAT configuration as its configuration should be right as first need to bring BGP up)

```
interface Serial0/0/1
description Link to ISP
ip address 209.65.200.225 255.255.255.252
ip access-group edge_security in
ip virtual-reassembly
ntp broadcast client
ntp broadcast key 1
no cdp enable
```

```
ip nat inside source list nat_traffic interface Serial0/0/1 overload
ip access-list standard nat_traffic
permit 10.1.0.0 0.0.255.255
permit 10.2.0.0 0.0.255.255
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
permit ip host 209.65.200.241 any
```

- In above snapshot we can see that access-list of edge_security on R1 is not allowing wan IP network- Change required: On R1, we need to permit IP 209.65.200.222/30 under the access list.

QUESTION 56The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located? A. R1B. R2C. R3D. R4E. DSW1F. DSW2G. ASW1

Answer: A
Explanation: On R1, we need to permit IP 209.65.200.222/30 under the access list.

QUESTION 57The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology? A. BGPB. NTPC. IP NATD. IPv4 OSPF RoutingE. IPv4 OSPF RedistributionF. IPv6 OSPF RoutingG. IPv4 layer 3 security

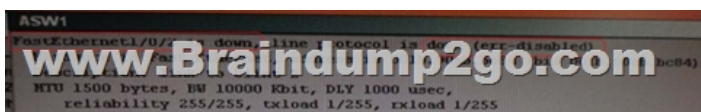
Answer: G
Explanation: On R1, we need to permit IP 209.65.200.222/30 under the access list.

QUESTION 58The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition? A. Under the interface Serial0/0/1 enter the ip access-group edge_security out command.B. Under the ip access-list extended edge_security configuration add the permit ip 209.65.200.224 0.0.0.3 any command.C. Under the ip access-list extended edge_security configuration delete the deny ip 10.0.0.0 0.255.255.255 any command.D. Under the interface Serial0/0/0 configuration delete the ip access-group edge_security in command and enter the ip access-group edge_security out command.

Answer: B
Explanation: On R1, we need to permit IP 209.65.200.222/30 under the access list.

Ticket 7 : Port SecurityTopology Overview (Actual Troubleshooting lab design is for below network design)- Client Should have IP 10.2.1.3- EIGRP 100 is running between switch DSW1 & DSW2- OSPF (Process ID 1) is running between R1, R2, R3, R4- Network of OSPF is redistributed in EIGRP- BGP 65001 is configured on R1 with Webserver cloud AS 65002- HSRP is running between DSW1 & DSW2 SwitchesThe company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches. In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary. R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range. R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network. ASW1 and ASW2 are layer 2 switches. NTP is enabled on all devices with 209.65.200.226 serving as the master clock source. The client workstations receive their IP address and default gateway via R4's DHCP server. The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2. In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing

domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary. Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations. Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution. Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device, Question-2 Fault condition is related to, Question-3 What exact problem is seen & what needs to be done for solution Client is unable to ping IP 209.65.200.241 Solution: Steps need to follow as below:- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig ---- Client will be getting 169.X.X.X- On ASW1 port Fa1/0/1 & Fa1/0/2 access port VLAN 10 was assigned but when we checked interface it was showing down Sh run ----- check for running config of int fa1/0/1 & fa1/0/2 (switchport access Vlan 10 will be there with switchport security command). Now check as below Sh int fa1/0/1 & sh int fa1/0/2



- As seen on interface the port is in err-disable mode so need to clear port. - Change required: On ASW1, for port security need command to remove port-security under interface under interface fa1/0/1 & fa1/0/2. QUESTION 59 The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolate the cause of this fault and answer the following questions. On which device is the fault condition located? A. R1 B. R2 C. R3 D. R4 E. DSW1 F. DSW2 G. ASW1 H. ASW2 Answer: G Explanation: port security needs is configured on ASW1. QUESTION 60 The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolate the cause of this fault and answer the following questions. The fault condition is related to which technology? A. NTP B. Switch-to-Switch Connectivity C. Access Vlan D. Port Security E. VLAN ACL / Port ACL F. Switch Virtual Interface Answer: D Explanation: Port security is causing the connectivity issues. On ASW1, we need to remove port-security under interface fa1/0/1 & fa1/0/2. QUESTION 61 The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolate the cause of this fault and answer the following questions. What is the solution to the fault condition? A. In Configuration mode, using the interface range Fa 1/0/1 - 2, then no switchport port- security interface configuration commands. Then in exec mode clear errdisable interface fa 1/0/1 - 2 vlan 10 command B. In Configuration mode, using the interface range Fa 1/0/1 - 2, then no switchport port- security, followed by shutdown, no shutdown interface configuration commands. C. In Configuration mode, using the interface range Fa 1/0/1 - 2, then no switchport port- security interface configuration commands. D. In Configuration mode, using the interface range Fa 1/0/1 - 2, then no switchport port- security interface configuration commands. Then in exec mode clear errdisable interface fa 1/0/1, then clear errdisable interface fa 1/0/2 commands. Answer: B Explanation: On ASW1, we need to remove port-security under interface fa1/0/1 & fa1/0/2. http://www.cisco.com/en/US/tech/ABC389/ABC621/technologies_tech_note09186a00806cd87b.shtml Ticket 8 : Redistribution of EIGRP to OSPF Topology Overview (Actual Troubleshooting lab design is for below network design)- Client Should have IP 10.2.1.3- EIGRP 100 is running between switch DSW1 & DSW2- OSPF (Process ID 1) is running between R1, R2, R3, R4- Network of OSPF is redistributed in EIGRP- BGP 65001 is configured on R1 with Webserver cloud AS 65002- HSRP is running between DSW1 & DSW2 Switches The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches. In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10.

Redistribution is enabled where necessary. R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range. R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network. ASW1 and ASW2 are layer 2 switches. NTP is enabled on all devices with 209.65.200.226 serving as the master clock source. The client workstations receive their IP address and default gateway via R4's DHCP server. The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2. In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary. Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations. Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution. Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device, Question-2 Fault condition is related to, Question-3 What exact problem is seen & what needs to be done for solution. Client is unable to ping IP 209.65.200.241. Solution: Steps need to follow as below:- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig ----- Client will be receiving IP address 10.2.1.3- IP 10.2.1.3 will be able to ping from R4, but cannot ping from R3, R2, R1- This clearly shows problem at R4 since EIGRP is between DSW1, DSW2 & R4 and OSPF protocol is running between R4, R3, R2, R1 so routes from R4 are not propagated to R3, R2, R1- Since R4 is able to ping 10.2.1.3 it means that routes are received in EIGRP & same needs to be advertised in OSPF to ping from R3, R2, R1.- Need to check the routes are being advertised properly or not in OSPF & EIGRP vice-versa.

```
router eigrp 10
 redistribute ospf 1 route-map OSPF_to_EIGRP
 network 10.1.4.0 0.0.0.255
 network 10.1.10.0 0.0.0.255
 network 10.1.21.128 0.0.0.3
 default-metric 100000 100 100 1 1500
www.Braindump2go.com
router ospf 1
 log-adjacency-changes
 area 34 nssa
 summary-address 10.2.0.0 255.255.0.0
 redistribute eigrp 10 subnets route-map EIGRP->OSPF
 network 10.1.1.0 0.0.0.255 area 34
 network 10.1.2.0 0.0.0.255 area 34
```

```
route-map EIGRP->OSPF deny 10
 match tag 110
!
route-map EIGRP->OSPF permit 20
 match tag 90
www.Braindump2go.com
route-map OSPF->EIGRP deny 10
 match tag 90
!
route-map OSPF->EIGRP permit 20
```

- From above snap shot it clearly indicates that redistribution done in EIGRP is having problem & by default all routes are denied from ospf to EIGRP... so need to change route-map name.- Change required: On R4, in redistribution of EIGRP routing protocol, we need to change name of route-map to resolve the issue...QUESTION 62The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address. Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located? A. R1B. R2C. R3D. R4E. DSW1F. DSW2G. ASW1H. ASW2Answer: DExplanation: On R4, in the redistribution of EIGRP routing protocol, we need to change name of route- map to resolve the issue. It references route-map OSPF_to_EIGRP but the actual route map is called OSPF->EIGRP.!!!RECOMMEND!!!1.[2017 New 300-135 Exam Dumps (PDF & VCE) 131Q&As Download: <https://www.braindump2go.com/300-135.html>2.[2017 New 300-135 Study Guide Video: YouTube Video:

[YouTube.com/watch?v=5ShhGW0k1VA](https://www.youtube.com/watch?v=5ShhGW0k1VA)