Configuring OSPF Authentication on a Virtual Link

Document ID: 8313

Contents

Introduction

All areas in an Open Shortest Path First (OSPF) autonomous system must physically connect to the backbone area (area 0). However, in cases where this physical connection is not possible, you can use a virtual link to connect to the backbone through a nonbackbone area. You can also use virtual links to connect two parts of a partitioned backbone through a nonbackbone area. You can also enable OSPF authentication on virtual links.

This document describes how to enable plain text and Message Digest 5 (MD5) authentication on a virtual link in an OSPF network. Refer to Sample Configuration for Authentication in OSPF for more information on how to configure OSPF authentication.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of OSPF routing protocol and its operations
- Knowledge of OSPF virtual links concept

For more information on OSPF routing protocol and the concept of virtual links in OSPF, refer to OSPF Design Guide.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2500 Series Routers
- Cisco IOS® Software Release 12.2(27)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:
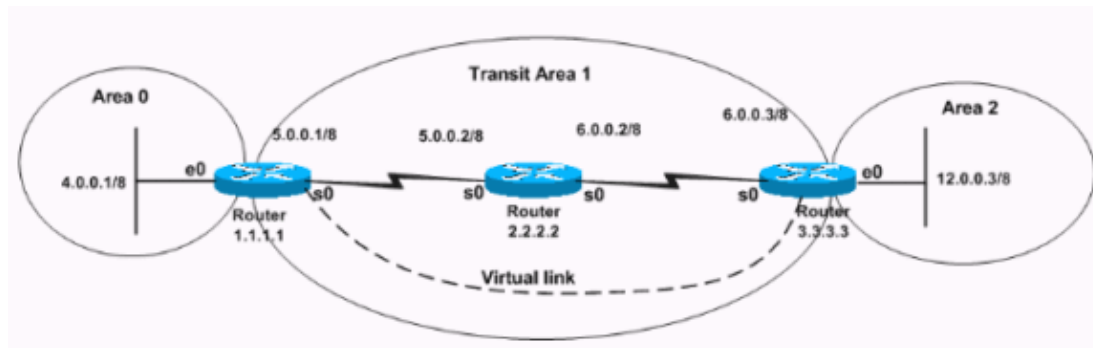
Configurations

This document uses these configurations:

- Configure Plain Text Authentication
- Configure MD5 Authentication

Configure Plain Text Authentication

Plain text authentication sends the passwords through the network as clear text. In this configuration, Router 3.3.3.3 has no interface in area 0, but connects virtually to area 0. This configuration makes Router 3.3.3.3 a virtual Area Border Router (ABR), so you must enable authentication for area 0 on Router 3.3.3.3. This section provides the commands to configure plain text authentication in a virtual link scenario.

Note: The authentication key that the configuration uses defines the key (the password) that is inserted directly into the OSPF header. The key is inserted into the header when the Cisco IOS Software originates routing protocol packets. You can assign a separate password to each network on a per−interface basis. All neighboring routers on the same network must have the same password in order to exchange OSPF information.

Router 1.1.1.1
`hostname r1.1.1.1`

```
interface Loopback0
 ip address 1.1.1.1 255.0.0.0

interface Ethernet0
 ip address 4.0.0.1 255.0.0.0
 ip ospf authentication-key cisco

!--- This command configures the authentication key (password)
!--- on the interface as "cisco".


interface Serial0
 ip address 5.0.0.1 255.0.0.0
 clockrate 64000

!

 router ospf 2
 network 4.0.0.0 0.255.255.255 area 0
 network 5.0.0.0 0.255.255.255 area 1
 area 0 authentication

!--- This command enables plain authentication for area 0
!--- on the router.

area 1 virtual-link 3.3.3.3 authentication-key cisco

!--- This command creates the virtual link between Router
!--- 1.1.1.1 and Router 3.3.3.3 with plain text authentication enabled.
```

Router 3.3.3.3

```
hostname r3.3.3.3

interface Loopback0
 ip address 3.3.3.3 255.0.0.0

interface Ethernet0
 ip address 12.0.0.3 255.0.0.0

interface Serial0
 ip address 6.0.0.3 255.0.0.0

!

 router ospf 2
 network 12.0.0.0 0.255.255.255 area 2
 network 6.0.0.0 0.255.255.255 area 1
 area 0 authentication

!--- This command enables plain authentication for area 0
!--- on the router.

 area 1 virtual-link 1.1.1.1 authentication-key cisco

!--- This command creates the virtual link to area 0 via
!--- transit area 1 with plain text authentication enabled.
```

Configure MD5 Authentication

MD5 authentication provides better security than plain text authentication. The security is better because this method uses the MD5 algorithm in order to compute a hash value from the contents of the OSPF packet and a password (or key). This hash value is transmitted in the packet, along with a key ID and a nondecreasing sequence number. The receiver, which knows the same password, calculates its own hash value. This section provides the commands to configure MD5 authentication in a virtual link scenario.

Router 1.1.1.1

```
hostname r1.1.1.1

interface Loopback0
 ip address 1.1.1.1 255.0.0.0

interface Ethernet0
 ip address 4.0.0.1 255.0.0.0
 ip ospf message-digest-key 1 md5 cisco

!--- This command configures the MD5 authentication key
!--- on the interface as "cisco".

interface Serial0
 ip address 5.0.0.1 255.0.0.0
 clockrate 64000

!

 router ospf 2
 network 4.0.0.0 0.255.255.255 area 0
 network 5.0.0.0 0.255.255.255 area 1
 area 0 authentication message-digest

!--- This command enables MD5 authentication for area 0
!--- on the router.

 area 1 virtual-link 3.3.3.3 message-digest-key 1 md5 cisco

!--- This command creates the virtual link between Router
!--- 1.1.1.1 and Router 3.3.3.3 with MD5 authentication enabled.
```

Router 3.3.3.3

```
hostname r3.3.3.3

interface Loopback0
 ip address 3.3.3.3 255.0.0.0

interface Ethernet0
 ip address 12.0.0.3 255.0.0.0

interface Serial0
 ip address 6.0.0.3 255.0.0.0

!

 router ospf 2
 network 12.0.0.0 0.255.255.255 area 2
 network 6.0.0.0 0.255.255.255 area 1
area 0 authentication message-digest

!--- This command enables MD5 authentication for area 0
!--- on the router.
```

```
area 1 virtual-link 1.1.1.1 message-digest-key 1 md5 cisco

!--- This command creates the virtual link to area 0 via
!--- the transit area 1 with MD5 authentication enabled.
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show ip ospf virtual−links** Displays parameters and the current state of OSPF virtual links.
- **show ip route** Displays the current state of the routing table.

Sample show Command Output Configure Plain Text Authentication

```
r3.3.3.3# show ip ospf virtual-links

Virtual Link OSPF_VL0 to router 1.1.1.1 is up

!--- The status of the virtual link displays.

  Run as demand circuit
  DoNotAge LSA allowed

!--- This specifies that OSPF runs as a demand circuit over virtual links,
!--- and so link-state advertisements (LSAs) are not refreshed (not aged out).

  Transit area 1, via interface Serial0, Cost of using 128
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
    Adjacency State FULL (Hello suppressed)

!--- The status of the neighbor adjacency displays.

    Index 1/2, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
  Simple password authentication enabled

!--- The type of authentication that is enabled displays.
!--- The authentication type is simple password.

r3.3.3.3#
```

Note: The output shows that OSPF hellos are suppressed. This means that, once the virtual link is up, no hellos are exchanged. OSPF suppresses the hellos because it considers virtual links to be demand circuits. Normally, OSPF sends hellos every 10 seconds and refreshes its LSAs every 30 minutes. However, even this amount of traffic is undesirable on demand circuits. The use of OSPF demand circuit options suppresses hello and LSA−refresh functions. As a result, any changes that you make to the OSPF authentication do not take effect until you clear the OSPF process with the **clear ip ospf process** command. An example is a change of the authentication type on the routers.

```
r3.3.3.3# show ip route
```

```
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP
       D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
       N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
       E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
       i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, ia – IS-IS inter area
       * – candidate default, U – per-user static route, o – ODR
       P – periodic downloaded static route
Gateway of last resort is not set
C 3.0.0.0/8 is directly connected, Loopback0
O 4.0.0.0/8 [110/138] via 6.0.0.2, 00:31:08, Serial0
O 5.0.0.0/8 [110/128] via 6.0.0.2, 22:55:44, Serial0
C 6.0.0.0/8 is directly connected, Serial0
C 12.0.0.0/8 is directly connected, Ethernet0
r3.3.3.3#
```

Sample show Command Output Configure MD5 Authentication

```
r3.3.3.3# show ip ospf virtual-links

Virtual Link OSPF_VL1 to router 1.1.1.1 is up

!--- The status of the virtual link displays.

  Run as demand circuit
  DoNotAge LSA allowed

!--- This specifies that OSPF runs as a demand circuit over virtual links,
!--- and so LSAs are not refreshed (not aged out).

  Transit area 1, via interface Serial0, Cost of using 128
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
    Adjacency State FULL (Hello suppressed)

!--- The status of the neighbor adjacency displays.

    Index 1/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
  Message digest authentication enabled

!--- The type of authentication that is enabled displays.
!--- The authentication type is MD5.

    Youngest key id is 1

r3.3.3.3# show ip route

Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP
       D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
       N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
       E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
       i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, ia – IS-IS inter area
       * – candidate default, U – per-user static route, o – ODR
       P – periodic downloaded static route
Gateway of last resort is not set
C 3.0.0.0/8 is directly connected, Loopback0
O 4.0.0.0/8 [110/138] via 6.0.0.2, 00:02:41, Serial0
O 5.0.0.0/8 [110/128] via 6.0.0.2, 00:02:51, Serial0
C 6.0.0.0/8 is directly connected, Serial0
C 12.0.0.0/8 is directly connected, Ethernet0
```

Troubleshoot

Use this section to troubleshoot your configuration.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug ip ospf adj** Debugs the OSPF neighbor adjacency establishment process.

Sample debug Command Output Configure Plain Text Authentication

```
r3.3.3.3# debug ip ospf adj

23:31:41: OSPF: Interface OSPF_VL0 going Up
23:31:41: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x8000002E
23:31:41: OSPF: Build router LSA for area 1, router ID 3.3.3.3, seq 0x8000002E
23:31:41: OSPF: Build router LSA for area 2, router ID 3.3.3.3, seq 0x80000031
23:31:51: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL0 seq 0x887 opt 0x62 flag 0x7
 len 32  mtu 0 state INIT
23:31:51: OSPF: 2 Way Communication to 1.1.1.1 on OSPF_VL0, state 2WAY
23:31:51: OSPF: Send DBD to 1.1.1.1 on OSPF_VL0 seq 0x2102 opt 0x62 flag 0x7 len 32
23:31:51: OSPF: First DBD and we are not SLAVE
23:31:51: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL0 seq 0x2102 opt 0x62 flag 0x2
 len 172  mtu 0 state EXSTART
23:31:51: OSPF: NBR Negotiation Done. We are the MASTER
23:31:51: OSPF: Send DBD to 1.1.1.1 on OSPF_VL0 seq 0x2103 opt 0x62 flag 0x3 len 172
23:31:51: OSPF: Database request to 1.1.1.1
23:31:51: OSPF: sent LS REQ packet to 5.0.0.1, length 12
23:31:51: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL0 seq 0x2103 opt 0x62 flag 0x0 len 32
 mtu 0 state EXCHANGE
23:31:51: OSPF: Send DBD to 1.1.1.1 on OSPF_VL0 seq 0x2104 opt 0x62 flag 0x1 len 32
23:31:51: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL0 seq 0x2104 opt 0x62 flag 0x0
 len 32  mtu 0 state EXCHANGE
23:31:51: OSPF: Exchange Done with 1.1.1.1 on OSPF_VL0
23:31:51: OSPF: Synchronized with 1.1.1.1 on OSPF_VL0, state FULL

!--- This indicates the establishment of neighbor adjacency.

23:31:51: %OSPF-5-ADJCHG: Process 2, Nbr 1.1.1.1 on OSPF_VL0 from LOADING to FULL,
 Loading Done
23:31:52: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x8000002F
23:32:23: OSPF: Dead event ignored for 1.1.1.1 on demand circuit OSPF_VL0
r3.3.3.3#
```

Sample debug Command Output Configure MD5 Authentication

```
r3.3.3.3# debug ip ospf adj

23:48:06: OSPF: Interface OSPF_VL1 going Up
23:48:06: OSPF: Send with youngest Key 0
23:48:07: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x80000001
23:48:07: OSPF: Build router LSA for area 2, router ID 3.3.3.3, seq 0x80000033
23:48:07: OSPF: Build router LSA for area 1, router ID 3.3.3.3, seq 0x80000030
23:48:14: OSPF: 2 Way Communication to 1.1.1.1 on OSPF_VL1, state 2WAY
23:48:14: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x7 len32
23:48:14: OSPF: Send with youngest Key 1
23:48:14: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x3FB opt 0x62 flag 0x7
 len 32 mtu 0 state EXSTART
23:48:14: OSPF: First DBD and we are not SLAVE
23:48:16: OSPF: Send with youngest Key 1
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x7 len 32
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Retransmitting DBD to 1.1.1.1 on OSPF_VL1 [1]
```

```
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x3FB opt 0x62 flag 0x7 len 32
 mtu 0 state EXSTART
23:48:19: OSPF: First DBD and we are not SLAVE
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x2
 len 172 mtu 0 state EXSTART
23:48:19: OSPF: NBR Negotiation Done. We are the MASTER
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EB opt 0x62 flag 0x3 len 112
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Database request to 1.1.1.1
23:48:19: OSPF: sent LS REQ packet to 5.0.0.1, length 48
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EB opt 0x62 flag 0x0 len 32
 mtu 0 state EXCHANGE
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EC opt 0x62 flag 0x1 len 32
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x80000030
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EC opt 0x62 flag 0x0 len 32
 mtu 0 state EXCHANGE
23:48:19: OSPF: Exchange Done with 1.1.1.1 on OSPF_VL1
23:48:19: OSPF: Synchronized with 1.1.1.1 on OSPF_VL1, state FULL

!--- This indicates the establishment of neighbor adjacency.

23:48:19: %OSPF-5-ADJCHG: Process 2, Nbr 1.1.1.1 on OSPF_VL1 from LOADING to FULL,
 Loading Done
```

Related Information

- **OSPF Support Page**
- **OSPF Design Guide**
- **OSPF Virtual Link**
- **Sample Configuration for Authentication in OSPF**
- **OSPF Demand Circuit Feature**
- **Technical Support & Documentation – Cisco Systems**