Configure IS-IS Authentication

Contents

Introduction

This document describes the configuration of the authentication for routing protocols in order to prevent the introduction of malicious information into the routing table. This document demonstrates clear text authentication between routers running Intermediate System-to-Intermediate System (IS-IS) for IP.

This document only covers the IS-IS Clear Text Authentication. Refer to Enhancing Security in an IS-IS Network for more information about the other types of IS-IS authentication.

Prerequisites

Requirements

Readers of this document should be familiar with IS-IS operation and configuration.

Components Used

This document is not restricted to specific software and hardware versions. The configuration in this document was tested on Cisco 2500 series routers, running Cisco IOS version 12.2(24a).

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, ensure that you understand the potential impact of any command.

Background Information

IS-IS allows for the configuration of a password for a specified link, an area, or a domain. Routers that want to become neighbors must exchange the same password for their configured level of authentication. A router

not in possession of the appropriate password is prohibited from participating in the corresponding function (that is, it may not initialize a link, be a member of an area, or be a member of a Level 2 domain, respectively).

Cisco IOS® software allows three types of IS-IS authentication to be configured.

- **IS-IS Authentication** - For a long time, this was the only way to configure authentication for IS-IS.
- **IS-IS HMAC-MD5 Authentication** - This feature adds an HMAC-MD5 digest to each IS-IS protocol data unit (PDU). It was introduced in Cisco IOS software version 12.2(13)T and is only supported on a limited number platforms.
- **Enhanced Clear Text Authentication** - With this new feature, clear text authentication can be configured using new commands that allow passwords to be encrypted when the software configuration is displayed. It also makes passwords easier to manage and change.

Note: Refer to Enhancing Security in an IS-IS Network for information on ISIS MD-5 and Enhanced Clear Text Authentication.

The IS-IS protocol, as specified in RFC 1142, provides for the authentication of Hellos and Link State Packets (LSPs) through the inclusion of authentication information as part of the LSP. This authentication information is encoded as a Type Length Value (TLV) triple. The type of the authentication TLV is 10; the length of the TLV is variable; and the value of the TLV depends on the authentication type being used. By default, authentication is disabled.

Configure

This section discusses how to configure IS-IS clear text authentication on a link, for an Area and for a Domain.

Interface Authentication

When you configure IS-IS authentication on an interface, you can enable the password for Level 1, Level 2, or both Level 1/Level 2 routing. If you do not specify a level, the default is Level 1 and Level 2. Depending on the level for which authentication is configured, the password is carried in the corresponding Hello messages. The level of IS-IS interface authentication should track the type of adjacency on the interface. Use the **show clns neighbor** command to find out the type of adjacency. For area and domain authentication, you cannot specify the level.

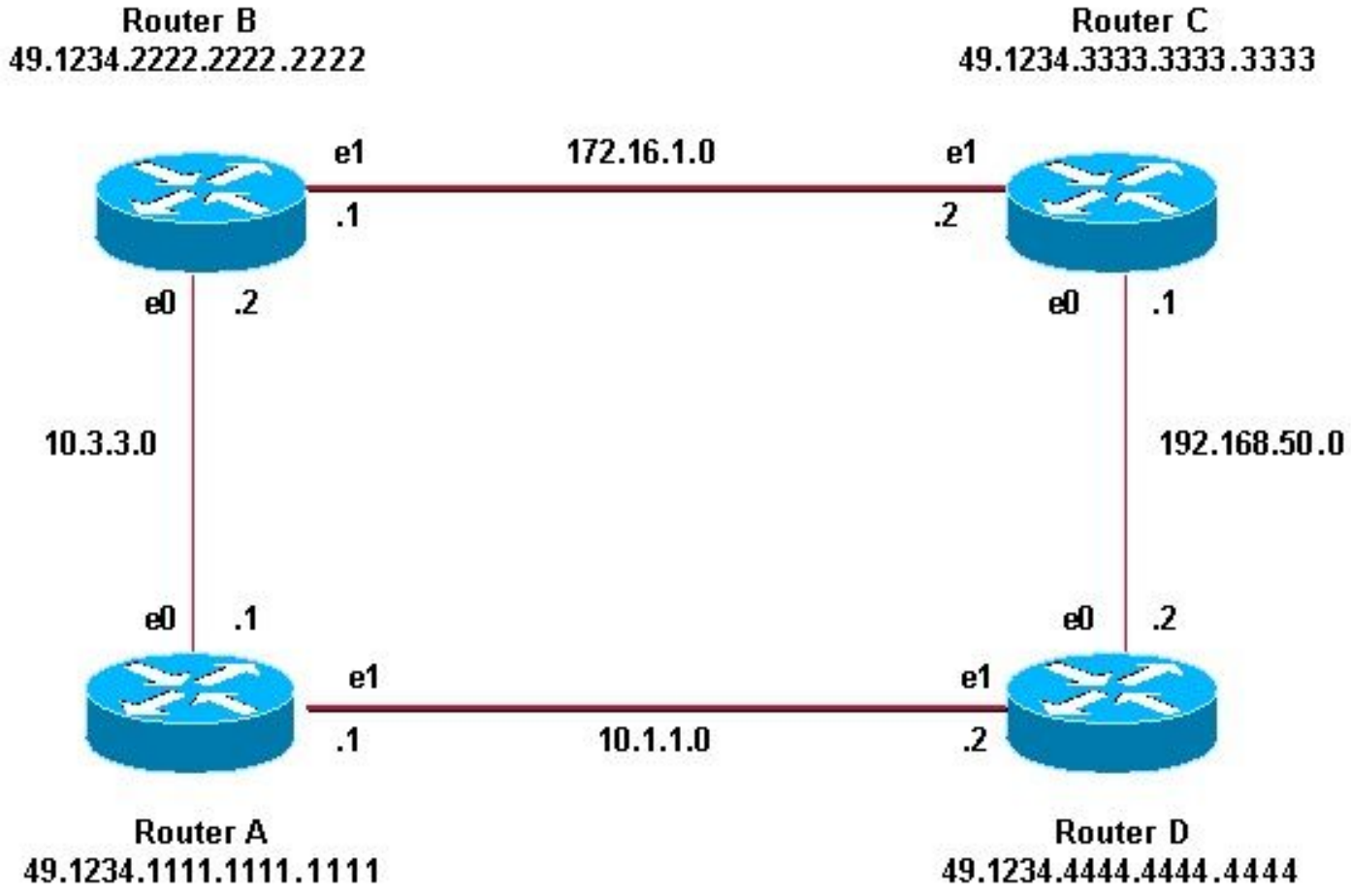
The network diagram and configurations for interface authentication on Router A, Ethernet 0 and Router B, Ethernet 0 are shown below. Router A and Router B are both configured with isis password SECr3t for both Level 1 and Level 2. These passwords are case sensitive.

On Cisco routers configured with Connectionless Network Service (CLNS) IS-IS, the CLNS adjacency between them is Level 1/Level 2 by default. So, Router A and Router B will have both types of adjacency, unless configured specifically for Level 1 or Level 2.

Router A	Router B
interface ethernet 0 ip address 10.3.3.1 255.255.255.0 ip router isis isis password SECr3t interface ethernet1 ip address 10.1.1.1 255.255.255.0 ip router isis router isis net 49.1234.1111.1111.1111.00	interface ethernet 0 ip address 10.3.3.2 255.255.255.0 ip router isis isis password SECr3t interface ethernet1 ip address 172.16.1.1 255.255.255.0 ip router isis router isis net 49.1234.2222.2222.2222.00

Area Authentication

The network diagram and configurations for area authentication are shown below. When area authentication is configured, the password is carried in the L1 LSPs, CSNPs and PSNPS. All of the routers are in the same IS-IS area, 49.1234, and they are all configured with the area password "tiGHter."



Router A	Router B
<#root> interface ethernet 0 ip address 10.3.3.1 255.255.255.0 ip router isis interface ethernet1	<#root> interface ethernet 0 ip address 10.3.3.2 255.255.255.0 ip router isis interface ethernet1

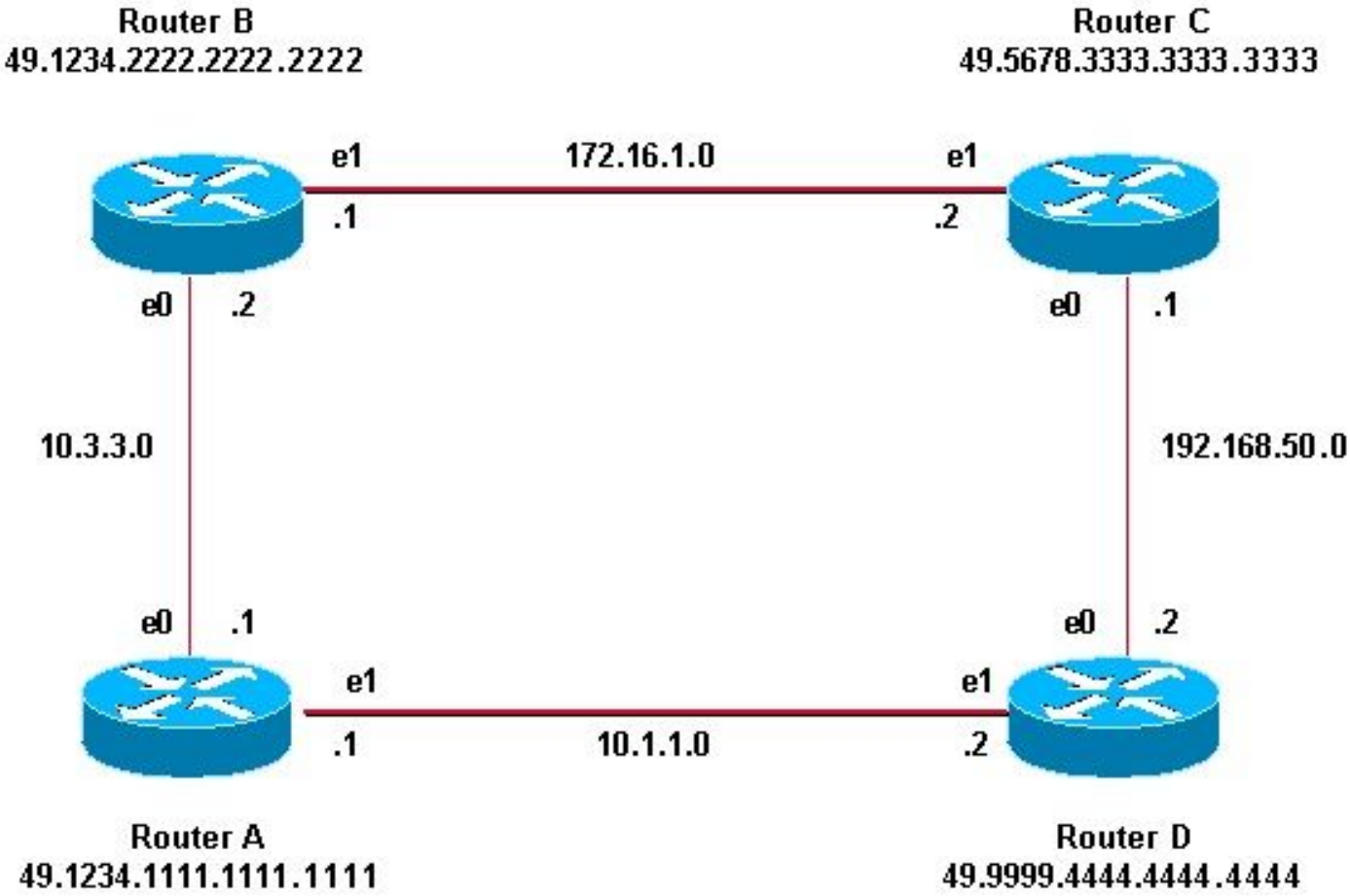
```
ip address 10.1.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.1111.1111.1111.00

area-password tiGHter
```

```
ip address 172.16.1.1 255.255.255.0
ip router isis

router isis
net 49.1234.2222.2222.2222.00

area-password tiGHter
```

Router C	Router D
<#root> interface ethernet1 ip address 172.16.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.1 255.255.255.0 ip router isis router isis net 49.1234.3333.3333.3333.00 **area-password tiGHter**	<#root> interface ethernet1 ip address 10.1.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.2 255.255.255.0 ip router isis router isis net 49.1234.4444.4444.4444.00 **area-password tiGHter**

Domain Authentication

The network diagram and configurations for domain authentication are shown below. Router A and Router B are in IS-IS area 49.1234; Router C is in IS-IS area 49.5678; and Router D is in area 49.9999. All of the routers are in the same IS-IS Domain (49) and are configured with the domain password "seCurity."



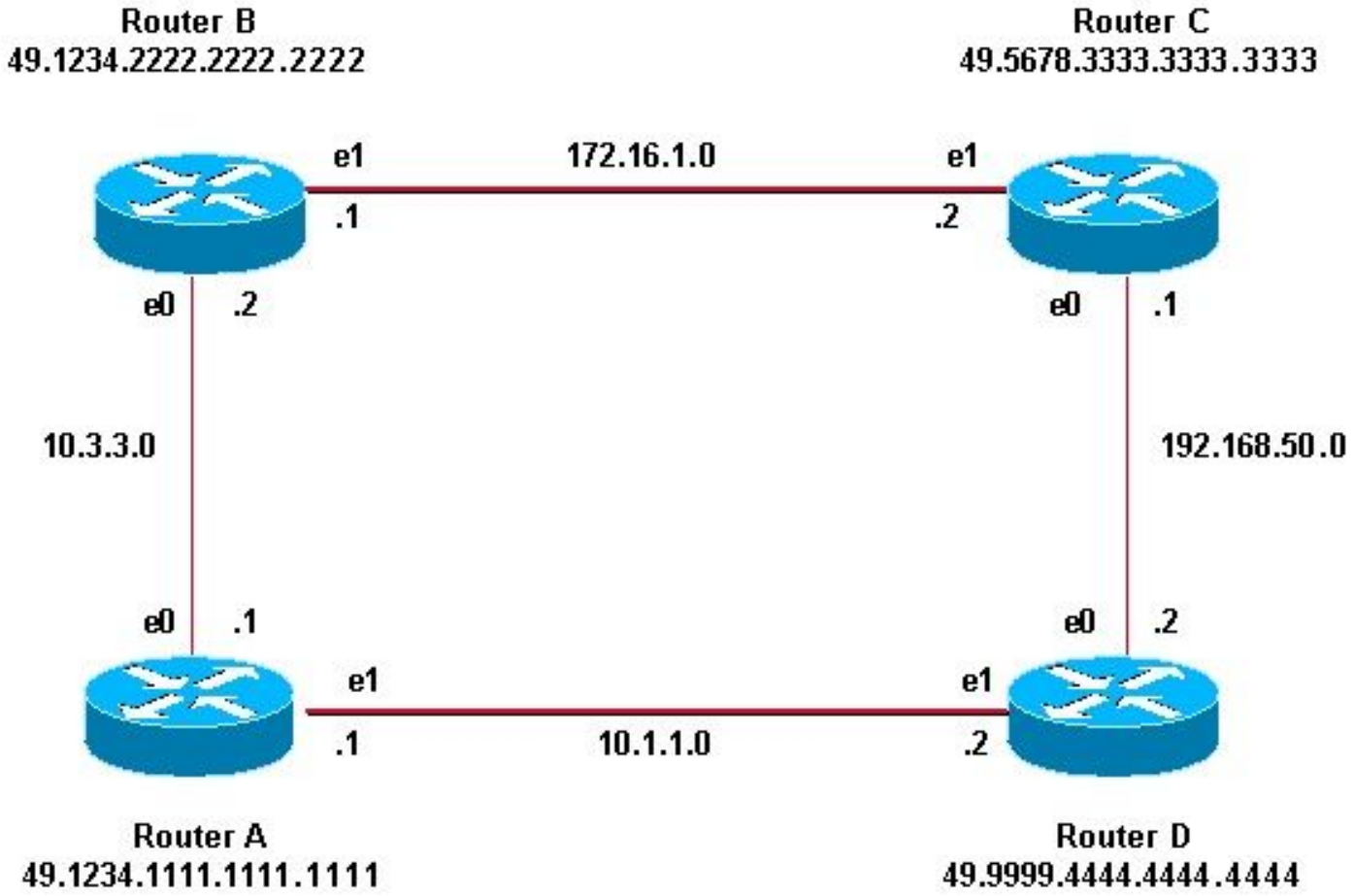
Router A	Router B
<#root> interface ethernet 0 ip address 10.3.3.1 255.255.255.0 ip router isis interface ethernet1 ip address 10.1.1.1 255.255.255.0 ip router isis router isis net 49.1234.1111.1111.1111.00 **domain-password seCurity**	<#root> interface ethernet 0 ip address 10.3.3.2 255.255.255.0 ip router isis interface ethernet1 ip address 172.16.1.1 255.255.255.0 ip router isis router isis net 49.1234.2222.2222.2222.00 **domain-password seCurity**

Router C	Router D
<#root> interface ethernet1 ip address 172.16.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.1 255.255.255.0 ip router isis router isis net 49.5678.3333.3333.3333.00	<#root> interface ethernet1 ip address 10.1.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.2 255.255.255.0 ip router isis router isis net 49.9999.4444.4444.4444.00

domain-password seCurity	**domain-password seCurity**

Combining Domain, Area, and Interface Authentication

The topology and partial configurations in this section illustrate a combination of domain, area, and interface authentication. Router A and Router B are in the same area and are configured with the area password "tiGHter." Router C and Router D belong to two different areas than Router A and Router B. All routers are in the same domain and share the domain-level password "seCurity." Router B and Router C have an interface configuration for the Ethernet link between them. Router C and Router D form only L2 adjacencies with their neighbors and configuring area password is not required.



Router A	Router B
<#root> interface ethernet 0 ip address 10.3.3.1 255.255.255.0 ip router isis interface ethernet1 ip address 10.1.1.1 255.255.255.0 ip router isis router isis net 49.1234.1111.1111.1111.00 **domain-password seCurity** **area-password tiGHter**	<#root> interface ethernet 0 ip address 10.3.3.2 255.255.255.0 ip router isis interface ethernet1 ip address 172.16.1.1 255.255.255.0 ip router isis clns router isis **isis password Fri3nd level-2** router isis

	net 49.1234.2222.2222.2222.00 **domain-passwordseCurity** **area-password tiGHter**

Router C	Router D
<#root> interface ethernet1 ip address 172.16.1.2 255.255.255.0 ip router isis **isis password Fri3nd level-2** interfaceethernet0 ip address 192.168.50.1 255.255.255.0 ip router isis router isis net 49.5678.3333.3333.3333.00 **domain-password seCurity**	<#root> interface ethernet1 ip address 10.1.1.2 255.255.255.0 ip router isis interface ethernet0 ip address 192.168.50.2 255.255.255.0 ip router isis router isis net 49.9999.4444.4444.4444.00 **domain-password seCurity**

Verify

Certain **show** commands are supported by the Cisco CLI Analyzer (registered customers only) , which allows you to view an analysis of **show** command output.

To verify if interface authentication is working properly, use the **show clns neighbors** command in the user EXEC or privileged EXEC mode. The output of the command displays the adjacency type and state of the connection. This sample output from the **show clns neighbors** command shows a router correctly configured for interface authentication and displays the state as UP:

<#root>

RouterA#

show clns neighbors

```
System Id      Interface   SNPA            State  Holdtime  Type Protocol
RouterB        Et0         0000.0c76.2882  Up     27        L1L2 IS-IS
```

For Area and Domain authentication, verification of authentication can be done using debug commands as explained in the next section.

Troubleshoot

If directly connected routers have authentication configured on one side of a link, and not on the other, the routers do not form a CLNS IS-IS adjacency. In the output below, Router B is configured for interface authentication on its Ethernet 0 interface, and Router A is not configured with authentication on its adjoining

interface.

```
<#root>

Router_A#

show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol

Router_B       Et0         00e0.b064.46ec      Init   265       IS   ES-IS


Router_B#

show clns neighbors
```

If directly connected routers have area-authentication configured on one side of a link, CLNS IS-IS adjacency is formed between the two routes. However, the router on which area-authentication is configured, does not accept L1 LSPs from the CLNS neighbor with no area-authentication configured. However, the neighbor with no area-authentication does continue to accept both L1 and L2 LSPs.

This is the debug message on Router A where area authentication is configured and receiving L1 LSP from a neighbor (Router B) without area authentication:

```
<#root>

Router_A#

deb isis update-packets

 IS-IS Update related packet debugging is on
 Router_A#
 *Mar 1 00:47:14.755: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1128,
 *Mar 1 00:47:14.759: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
 *Mar 1 00:47:14.763: ISIS-Upd:

LSP authentication failed

 Router_A#
 *Mar 1 00:47:24.455: ISIS-Upd: Rec L1 LSP 2222.2222.2222.00-00, seq 3, ht 1118,
 *Mar 1 00:47:24.459: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
 *Mar 1 00:47:24.463: ISIS-Upd:

LSP authentication failed

 RouterA#
```

If you configure domain authentication on one router, it rejects the L2 LSPs from routers that do not have domain authentication configured. Routers that do not have authentication configured accept the LSPs from the router that does have authentication configured.

The debug output below shows LSP authentication failures. Router CA is configured for area or domain authentication and is receiving Level 2 LSPs from a router (Router DB) which is not configured for domain or password authentication.

<#root>

```
Router_A#
```

debug isis update-packets

```
IS-IS Update related packet debugging is on
Router_A#
*Mar  1 02:32:48.315: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 374,
*Mar  1 02:32:48.319: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
*Mar  1 02:32:48.319: ISIS-Upd:
```

LSP authentication failed

```
Router_A#
*Mar  1 02:32:57.723: ISIS-Upd: Rec L2 LSP 2222.2222.2222.00-00, seq 8, ht 365,
*Mar  1 02:32:57.727: ISIS-Upd: from SNPA 0000.0c76.2882 (Ethernet0)
*Mar  1 02:32:57.727: ISIS-Upd:
```

LSP authentication failed

Related Information

- **IP Routing Support Page**
- **Technical Support & Documentation - Cisco Systems**