How To | Configure Common ISDN Access Concentration With The Firewall

Introduction

This How To Note provides examples of how to configure a network consisting of a number of remote Small Office / Home Office (SOHO) routers that connect to a central office router via ISDN connections. Three configurations are examined:

- First, a base example for when remote users dial into the central office router via ISDN.
- Second, additional complexity is added to improve security, such as firewall and packet filtering. This prevents remote offices from communicating with one another.
- Third, different authentication mechanisms are explored, using PPP-layer CHAP/PAP authentication via a RADIUS server, instead of ISDN-layer caller authentication.

What information will you find in this note?

The following three configurations are described:

Configuration 1—ISDN access concentration with the following characteristics:

- The remote users are authenticated at both the ISDN layer, via a CLI allow list and authenticated at the PPP layer via a PAP/CHAP username/password. This has the advantage that illegitimate calls are immediately dropped at the initial ISDN-layer authentication, reducing call costs. PPP-layer authentication follows a successful ISDN-layer authentication.
- The central site is unable to make outbound ISDN calls.
- The remote office routers are allocated pre-defined IP addresses. This means that the IP address for the remote office router should always remain fixed.

Configuration 2—ISDN access concentration and firewall:

- All of the features in configuration 1 are still present.
- Remote users are prevented from communicating with one another via software based IP packet filtering. Filtering is performed on received packets.
- Firewall is configured on the central office appliance.

Configuration 3—ISDN access concentration without ISDN layer call authentication (Cisco equivalent):

- ISDN call authentication by CLI is removed.
- IP assignment via a RADIUS server implemented.

Which products does it apply to?

This Note applies to the following Allied Telesis routers and managed layer 3 switches, running software version 2.4.1 or later:

- AR300, AR400, and AR700 series routers
- Rapier and Rapier i series switches

Related How To Notes

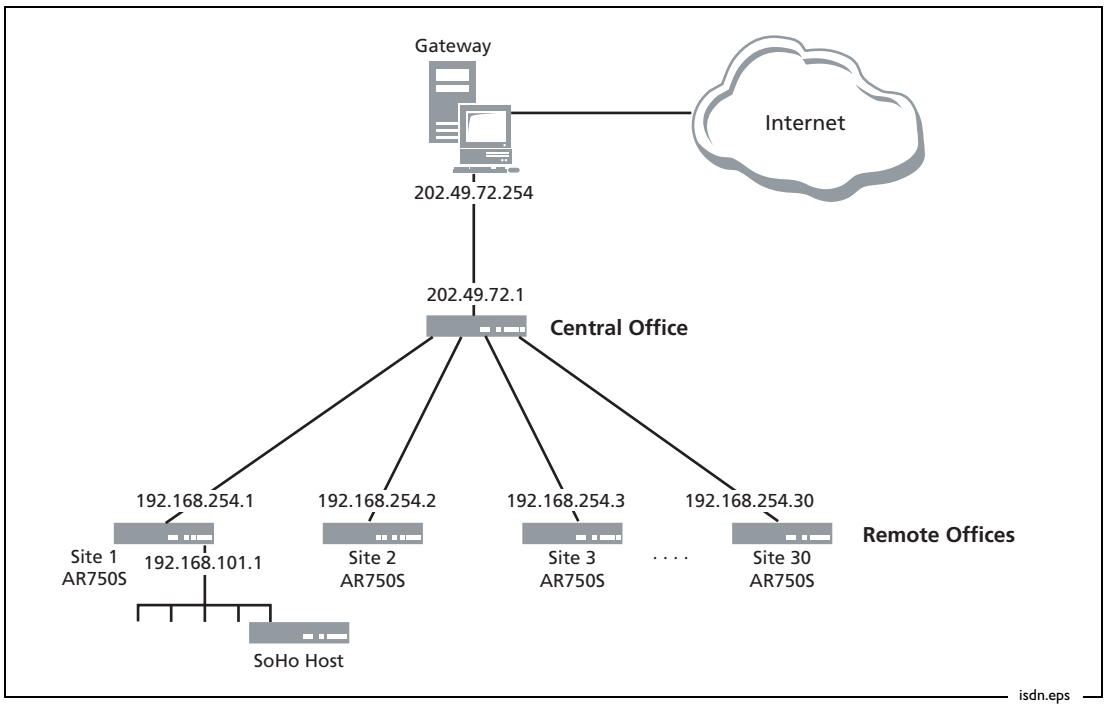
You may also find the following How To Notes useful:

- *How To Configure ISDN Calls On Allied Telesis Routers*
- *How To Configure Some Basic Firewall And VPN Scenarios*
- *How To Configure Some Advanced Features On Your ADSL Router*
- *How To Configure The Firewall Using The Graphical User Interface (GUI)*
- *How To Apply Firewall Policies And Rules*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

Network specification

The basic configuration consists of a central office router providing 30 ISDN BRI connections to 30 remote offices. Each remote router uses the same ISDN number to dial into the central office router. The remote routers each have LANs connecting a few hosts, and the central router connects to the Internet via a gateway.



Configuration 1—Basic ISDN access concentration

1. Configure the central office

```
set system name="Central_Office"

set system territory=europe
```

Configure the user logins and passwords for the remote offices (ROs) 1-30 that they will need for authentication. Assign a fixed IP address for each remote office based on its own unique calling number e.g. 111111 or 222222 etc.

```
add user=siteRO1 pass=testsite1 login=no

set user=siteRO1 telnet=no ipaddr=192.168.254.1
   netmask=255.255.255.255

set user=siteRO1 callingnumber=111111


add user=siteRO2 pass=testsite2 login=no

set user=siteRO2 telnet=no ipaddr=192.168.254.2
   netmask=255.255.255.255

set user=siteRO2 callingnumber=222222
```

and so on...

```
add user=siteRO30 pass=testsiteRO30 login=no

set user=siteRO30 telnet=no ipaddr=192.168.254.30
   netmask=255.255.255.255

set user=siteRO30 callingnumber=303030
```

Set the ISDN up to only allow inward bound calls

```
add isdn call=site1 number=111111 precedence=in direction=in
   searchcli=yes

add isdn call=site2 number=222222 precedence=in direction=in
   searchcli=yes
```

and so on...

```
add isdn call=site30 number=303030 precedence=in direction=in
   searchcli=yes
```

Note: The **number** parameter specifies the ISDN number to add to the CLI list. This number is compared with the number in the CLI information element (IE) in incoming SETUP messages, when the ISDN call selected has options set which require a search of the CLI list. The comparison takes place from the right-most digit to the left, and stops when the shorter number has been checked. For example the number 3432114 in an incoming CLI IE would match CLI list numbers 2114, 3432114 and 03343211 4. This is because some exchanges remove any leading area codes and/or country code when supplying CLI information to the router to authenticate.

Create ppp interfaces over ISDN and require callers to authenticate.

```
create ppp=1 over=isdn-site1 idle=on bap=off lqr=off echo=on
   auth=chap

create ppp=2 over=isdn-site2 idle=on bap=off lqr=off echo=on
   auth=chap

create ppp=3 over=isdn-site3 idle=on bap=off lqr=off echo=on
   auth=chap
```

and so on...

```
create ppp=30 over=isdn-site30 idle=on bap=off lqr=off echo=on
   auth=chap
```

Configure IP and create a public IP address on eth0

```
enable ip

add ip interface=eth0 ip=202.49.72.1
```

Set IP addresses for the ppp interfaces (set to addressless)

```
add ip interface=ppp1 ip=0.0.0.0

add ip interface=ppp2 ip=0.0.0.0

add ip interface=ppp3 ip=0.0.0.0
```

and so on...

```
add ip interface=ppp30 ip=0.0.0.0
```

Setup static IP routes to the hosts on the remote office LANs.

The central office router will create dynamic host-specific interface routes to each dial-in host, based on the host-specific route allocated from user database. If remote routers are not running NAT, then static routes to remote LAN subnets will be required

Note: Dynamic routing protocols such as RIP/OSPF etc will keep expensive ISDN calls open unnecessarily!

```
add ip route=192.168.101.0 mask=255.255.255.0 interface=ppp1
   next=192.168.254.1

add ip route=192.168.102.0 mask=255.255.255.0 interface=ppp2
   next=192.168.254.2

add ip route=192.168.103.0 mask=255.255.255.0 interface=ppp3
   next=192.168.254.3
```

and so on...

```
add ip route=192.168.130.0 mask=255.255.255.0 interface=ppp30
   next=192.168.254.30
```

Create a default route out to the Internet via the gateway on a public interface

```
add ip route=0.0.0.0 interface=eth0 next=202.49.72.254
```

2. Configure a remote site

```
set system name="site_RO1"
set system territory=europe
```

Configure the ISDN interface and assign a calling number

```
set q931=bay0.bri0 num1=11111
```

Configure ISDN call configuration

```
add isdn call=central number=54321 precedence=out
set isdn call=central direction=out
set isdn call=central outcli=interface
```

Create a PPP interface over ISDN that will time out after 60 seconds if idle

```
create ppp=0 idle=60 over=isdn-central bap=off lqr=off echo=on
set ppp=0 bap=off iprequest=on username="siteRO1"
   password="testsite1"
```

IP configuration and a default route that goes out via the ppp0 interface

```
enable ip
enable ip remote
add ip interface=eth0 ip=192.168.101.1 mask=255.255.255.0
add ip interface=ppp0 ip=0.0.0.0
add ip route=0.0.0.0 mask=0.0.0.0 interface=ppp0 next=0.0.0.0
```

3. Configure another remote site

```
set system name="site_RO2"
set system territory=europe
```

Configure the ISDN bay and assign a calling number

```
set q931=bay0.bri0 num1=22222
```

Configure ISDN call configuration

```
add isdn call=central number=54321 precedence=out
set isdn call=central direction=out
set isdn call=central outcli=interface
```

Create a PPP interface over ISDN that will time out after 60 seconds if idle

```
create ppp=0 idle=60 over=isdn-central bap=off lqr=off echo=on
set ppp=0 bap=off iprequest=on username="siteRO2"
   password="testsite2"
```

IP configuration and a default route that goes out via the ppp0 interface

```
enable ip
enable ip remote
add ip interface=eth0 ip=192.168.102.1 mask=255.255.255.0
add ip interface=ppp0 ip=0.0.0.0
add ip route=0.0.0.0 mask=0.0.0.0 interface=ppp0 next=0.0.0.0
```

The remaining remote office sites can be configured similarly.

Configuration 2—ISDN access concentration with the addition of filtering and firewall

In this case we take the basic requirements from configuration 1 and add filtering to prevent the remote offices from communicating with one another. We also add the firewall to allow the remote offices secure access to the Internet via the central office.

4. Configure the Central Office

```
set system name="Central_Office"
set system territory=europe
```

Configure the user logins and passwords for the remote offices (ROs) 1-30 that they will need for authentication. Assign a fixed IP address for each remote office

```
add user=siteRO1 pass=testsite1 login=no priv=user
set user=siteRO1 telnet=no ipaddr=192.168.254.1
   netmask=255.255.255.255
set user=siteRO1 callingnumber=111111


add user=siteRO2 pass=testsite2 login=no priv=user
set user=siteRO2 telnet=no ipaddr=192.168.254.2
   netmask=255.255.255.255
set user=site RO2 callingnumber=222222
```

and so on...

```
add user=siteRO30 pass=testsiteRO30 login=no priv=user
set user=siteRO30 telnet=no ipaddr=192.168.254.30
   netmask=255.255.255.255
set user=siteRO30 callingnumber=303030
```

Set the ISDN up to only allow inward bound calls

```
add isdn call=site1 number=111111 precedence=in direction=in
   searchcli=yes
add isdn call=site2 number=222222 precedence=in direction=in
   searchcli=yes
```

and so on...

```
add isdn call=site30 number=303030 precedence=in direction=in
   searchcli=yes
```

Create PPP interfaces over ISDN and require callers to authenticate

```
create ppp=1 over=isdn-site1 idle=on bap=off lqr=off echo=on
   auth=chap
create ppp=2 over=isdn-site2 idle=on bap=off lqr=off echo=on
   auth=chap
create ppp=3 over=isdn-site3 idle=on bap=off lqr=off echo=on
   auth=chap
```

and so on...

```
create ppp=30 over=isdn-site30 idle=on bap=off lqr=off echo=on
   auth=chap
```

Configure IP

```
enable ip
```

Prevent routing between remote users using software based IP packet filters. An IP filter is added to block all packets that have a destination address range coincident with the remote offices.

Note: Each packet is checked against the filters in sequential order.

```
add ip filter=1 source=0.0.0.0 smask=0.0.0.0 dest=192.168.0.0
   dmask=255.255.0.0 act=exclude
add ip filter=1 source=0.0.0.0 action=include
```

Give a public IP address to eth0

```
add ip interface=eth0 ip=202.49.72.1
```

Apply the filters to the ppp interfaces only, note these filters apply to packets **received** at the central office.

```
add ip interface=ppp1 ip=0.0.0.0 filter=1
add ip interface=ppp2 ip=0.0.0.0 filter=1
add ip interface=ppp3 ip=0.0.0.0 filter=1
```

and so on...

```
add ip interface=ppp30 ip=0.0.0.0 filter=1
```

Set up static IP routes to the hosts on the Remote Office LANs.

```
add ip route=192.168.101.0 mask=255.255.255.0 interface=ppp1
   next=192.168.254.1

add ip route=192.168.102.0 mask=255.255.255.0 interface=ppp2
   next=192.168.254.2

add ip route=192.168.103.0 mask=255.255.255.0 interface=ppp3
   next=192.168.254.3
```

and so on...

```
add ip route=192.168.130.0 mask=255.255.255.0 interface=ppp30
   next=192.168.254.30
```

Create a default route out to the Internet via the gateway on a public interface

```
add ip route=0.0.0.0 interface=eth0 next=202.49.72.254
```

Configure the firewall. All interfaces to the Remote Offices are private and NAT the addresses for all packets traversing between the private and eth0 (public) interfaces.

```
enable firewall

create firewall policy="Internet"


add firewall policy="Internet" interface=ppp1 type=private

add firewall policy="Internet" interface=ppp2 type=private
```

and so on...

```
add firewall policy="Internet" interface=ppp30 type=private

add firewall policy="Internet" interface=eth0 type=public


add firewall policy="Internet" nat=enhanced interface=ppp1
   gblint=eth0

add firewall policy="Internet" nat=enhanced interface=ppp2
   gblint=eth0
```

and so on...

```
add firewall policy="Internet" nat=enhanced interface=ppp30
   gblint=eth0
```

5. Configure a remote site

```
set system name="site_RO1"

set system territory=europe
```

Configure ISDN bay and assign a calling number

```
set q931=bay0.bri0 num1=11111
```

Configure ISDN call configuration

```
add isdn call=central number=54321 precedence=out

set isdn call=central direction=out

set isdn call=central outcli=interface
```

Create a PPP interface over isdn that will time out after 60 seconds if idle

```
create ppp=0 idle=60 over=isdn-central bap=off lqr=off echo=on
set ppp=0 bap=off iprequest=on username="siteRO1"
   password="testsite1"
```

Configure IP

```
enable ip
enable ip remote
add ip interface=eth0 ip=192.168.101.1 mask=255.255.255.0
add ip interface=ppp0 ip=0.0.0.0
add ip route=0.0.0.0 mask=0.0.0.0 interface=ppp0 next=0.0.0.0
```

6. Configure a second remote site

```
set system name="site_RO2"
set system territory=europe
```

Configure ISDN bay and assign a calling number

```
set q931=bay0.bri0 num1=22222
```

Configure ISDN call configuration

```
add isdn call=central number=54321 precedence=out
set isdn call=central direction=out
set isdn call=central outcli=interface
```

Create a PPP interface over ISDN that will time out after 60 seconds if idle

```
create ppp=0 idle=60 over=isdn-central bap=off lqr=off echo=on
set ppp=0 bap=off iprequest=on username="siteRO2"
   password="testsite2"
```

Configure IP

```
enable ip
enable ip remote
add ip interface=eth0 ip=192.168.102.1 mask=255.255.255.0
add ip interface=ppp0 ip=0.0.0.0
add ip route=0.0.0.0 mask=0.0.0.0 interface=ppp0 next=0.0.0.0
```

The remaining remote office sites can be configured similarly.

7. Check the operation of the filters

Filter hits can be checked using the command:

```
show ip filter
```

An example output would look something like this:

```
IP filters
```

No.	Ent.	Source Port Dest.Port Type	Source Address Dest. Address Act/Pol/Pri	Source Mask Dest. Mask Logging	Session Prot.(T/C) Matches	Size
1	1	---- ---- General	Any 192.168.0.0 Exclude	Any 255.255.0.0 Off	---- Any	Any Any 10
	2	---- ---- General	Any Any Include	Any Any Off	---- Any	Any Any 60
	Requests:	70	Passes: 60	Fails: 10		

Configuration 3—Authentication variation: ISDN access concentration without ISDN-layer call authentication

In this case we take the basic requirements from configuration 1 and remove the ISDN-layer call authentication. A single call can be defined with the ISDN parameter **inany=on** which obviates the need for a CLI list. This means, however, that **all** incoming calls will be accepted and be validated against this single ISDN call definition. Each user can be authenticated via PPP-layer CHAP/PAP authentication (via a RADIUS server for example), and subsequently allocated an IP address by the RADIUS server. This example does not prevent remote users from communicating with one another. Note also that ISDN calls will be accepted and opened even if PPP PAP/CHAP authentication fails, which may result in an ISDN call charge.

▶ Configure the Central Office

```
set system name="Central Office"

create ppp template=1 auth=pap lqr=off echo=on bap=off
   login=radius


add isdn call=dialin number=0 direction=answer precedence=in
   user=ppp login=none inany=on ppptemplate=1

add radius server=202.49.72.2 secret=secret


enable ip
```

```
add ip interface=eth0 ip=202.49.72.1

add ip route=0.0.0.0 mask=0.0.0.0 interface=eth0
   next=202.49.72.254
```

When a device makes a PPP connection to the router/switch, it can request an IP address. There are several methods that the central office router can use to decide which IP address to allocate to the remote site. It can use an IP address configured on an entry in the user database, or an address from an IP pool, or it can ask a RADIUS server for an address, or obtain an address by reverse DNS lookup. When the address is allocated to the remote site, the central office will automatically create a route to that address, via the PPP interface on which the peer connected. But, what if there is a LAN on the far side of the PPP remote site, and it is necessary to **also** create a route to the subnet being used on that LAN? The way to instruct the central office to create such a route is to authenticate the peer by RADIUS, and have one or more "framed route" attributes defined on the peer's user entry on the RADIUS server. For FreeRADIUS, for example, this is achieved by creating an entry in the users file with the following syntax:

```
siteRO1 Password = "testsite1",

User Service Type = Framed User,

Framed Protocol = PPP,

Framed Address = 192.168.254.1,

Framed Netmask = 255.255.255.255,

Framed Route = "192.168.101.0/24"

Framed MTU = 1500
```

This will cause the central office to create a route to 192.168.101.0/255.255.255.0, with a next hop of 192.168.254.1, via the PPP interface on which the remote site is connected. The syntax of the Framed route attribute is defined in RFC 2865. Note that you can have more than one framed route defined for a single user, in which case the central office will create a route for each framed route.

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16083-00 REV B