

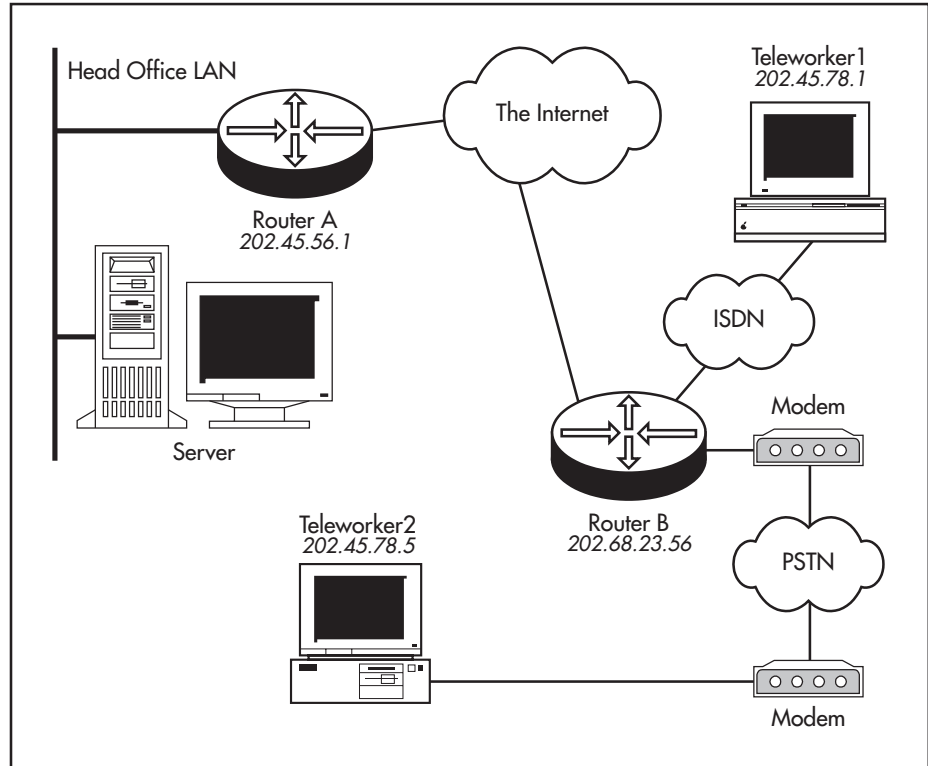
Configuration Example 19

Remote L2TP Tunnels

Companies wanting to allow teleworkers secure access to the company Head Office site face expensive telephone bills if the teleworkers are in another telephone districts. The solution is to locate a router in each telephone district to act as a clearing house for the teleworkers, and then connect that router via a Virtual Private Network (VPN) to a router at the Head Office site. The router at the Head Office site acts as the termination point for the remote VPN and the access point for the remote teleworker's traffic onto the Head Office site. The benefit is that the remote teleworker has access not only to the IP network, but also to any IPX networks operating at the Head Office site.

This example illustrates how to configure the AR router to allow ISDN and modem dial-up access for teleworkers to a central site. The configuration allows two-way communication, so that calls can be initiated from the Head Office site to a remote teleworker. The key to this configuration is that the Head Office router is configured with L2TP calls which create tunnels through the district router right out to the teleworkers. The calls are configured with a type and a call name. This tells the district router that when it receives a tunnel setup packet for that particular tunnel, it must activate the particular call of the specified type (asynchronous or ISDN) with the specified name, so that the tunnel can be established right out to the teleworker at the far end of that call. Note that the teleworkers do not need to be running any special software on their computers. As far as their computers are aware, this is a normal PPP session.

Figure 1: Setup Diagram



Configuration Script for Router A [ex19a.scp]

1. Set the system name. The prompt will change to "Manager Head Office>".

```
set sys name="Head Office"
```

2. Enable IP and assign an IP address to the Ethernet interface

```
enable ip
add ip int=eth0 ip=202.45.56.1
```

3. Create a PPP link to the ISP (assume here that it is a leased line connection), assign an IP address to the PPP interface and add a static route.

```
create ppp=0 over=syn0
add ip int=ppp0 ip=202.56.4.1
add ip route=0.0.0.0 int=ppp0 next=0.0.0.0
```

4. Enable L2TP and configure the router to act as both a LAC and a LNS.

```
enable l2tp
enable l2tp server=both
```

5. Set a password for verifying incoming L2TP tunnel setup requests

```
set l2tp password=verysecret
```

6. Create the L2TP call definition for teleworker 1, who is on an ISDN connection to the district router.

The parameters are:

- `ip` is the address of the district router terminates the ISDN call
- `type` indicates that it is an ISDN call that needs to be brought up to access the teleworker.

- `remote` specifies the name of the ISDN call that needs to be activated on the district router in order to access the teleworker.
- `password` is the password that will be checked by the district router when receiving the tunnel setup request.

```
add l2tp call=head-user1 type=isdn ip=202.68.23.56
    password=verysecret remote=tworke1
```

7. Create the L2TP call definition for teleworker 2, who is on an asynchronous connection to the district router. The parameters are:

- `ip` is the address of the district router terminates the asynchronous call.
- `type` indicates that it is an address call that needs to be brought up to access the teleworker.
- `remote` specifies the name of the address call that needs to be activated on the district router in order to access the teleworker.
- `password` is the password that will be checked by the district router when receiving the tunnel setup request.

```
add l2tp call=head-user2 type=async ip=202.68.23.56
    password=verysecret remote=tworke2
```

8. Create PPP links over the tunnels to the teleworkers. These are on-demand PPP links, so that when data needs to be sent to the teleworkers, the on-demand PPP will call on L2TP to open the relevant tunnel

```
create PPP=1 over=tnl-head-user1 idle=on
add ip int=ppp1 ip=202.45.78.2 mask=255.255.255.252
create PPP=2 over=tnl-head-user2 idle=on
add ip int=ppp2 ip=202.45.78.6 mask=255.255.255.252
```

9. In order to authenticate incoming calls from the teleworkers, the router stores their usernames and passwords.

```
add user=teleworker1 pass=password1
add user=teleworker2 pass=password2
```

Configuration Script for Router B [ex19b.scp]

1. Set the system name. The prompt will change to "Manager District>".

```
set sys name="District"
```

2. Enable IP and assign an IP address to the Ethernet interface

```
enable IP
add ip int=eth0 ip=202.68.23.56
```

3. Create a PPP link to the ISP (assume here that it is a leased line connection), assign an IP address to the PPP interface and add a static route.

```
create ppp=0 over=syn0
add ip int=ppp0 ip=187.4.45.2
add ip route=0.0.0.0 int=ppp0 next=0.0.0.0
```

4. Enable L2TP and configure the router to act as both a LAC and a LNS.

```
enable l2tp
enable l2tp server=both
```

5. Set a password for verifying incoming L2TP tunnel setup requests.

```
set l2tp password=verysecret
```

6. When the teleworkers dial in, they will receive CHAP challenges, to which they will respond with their usernames and passwords. These are sent to the Head Office router for authentication.

```
add l2tp user=all action=database ip=202.45.56.1
```

7. Create the asynchronous call on asynchronous port 1 of the router. The parameters on the ACC call definition are:

- `direction=both` means that this call definition will be used for incoming and outgoing calls.
- `encap=ppp` means that the data transport over this call will use PPP.
- `authen=chap` means that the router will send a CHAP challenge to the remote device as the PPP link opens.
- `port=1` means that the call definition is for asynchronous port 1
- `remote=head-user2` means that when this call definition is activated by an incoming call, the router sends an L2TP tunnel setup request to the Head Office router, asking it to open L2TP tunnel head-user2
- `dscr=ex19btw2.mds` means that when the call definition is activated in an outgoing direction, it must activate the modem dial script `ex19btw2.mds`

```
set port=1 flow=hardware speed=115200 cdc=connect
```

```
add acc call=tworker2 direction=both encap=ppp authen=chap
port=1 remote=head-user2 dscr=ex19btw2.mds
```

8. Create the ISDN call definition for teleworker 1 to call in via ISDN.

```
add isdn call=tworker1 num=8765321 prec=out
```

Dial Script `ex19btw2.mds` for Router B

1. Script `tworker2.mds` - modem dial script.

```
[ATDT678912^M]
```