Small Branch—Wireless Broadband Deployment

This chapter describes the use of wireless broadband service offerings for small office and home office (SOHO) deployments, including the documentation of the performance characteristics of encrypted voice over IP (VoIP) and the configuration of the remote router to use the services as either a primary or backup WAN.

This chapter includes the following sections:

- Solution Characteristics
- Topology
- Failover/Recovery Time
- Performance Results
- Wireless Broadband Hardware Components
- Verification
- Configuration
- Cisco IOS Versions Tested
- Caveats
- Summary

Solution Characteristics

This section describes the characteristics of the small branch wireless broadband deployment solution, and includes the following topics:

- Advantages
- Disadvantages

Advantages

DSL deployments require the phone line to be less than 2.5 miles from the central office of the carrier. To use cable, the residence must be serviced by a cable provider. Both these cases require physical wires, either twisted pair or coaxial cable. A primary advantage of wireless broadband is mobility; the ability to connect to the Internet without using a physical circuit.
Broadband wireless is ideal for a SOHO deployment when cable or DSL are not available, or when the lead time to install is inconvenient, as in the banking and hospitality sectors. Banks are commonly co-located in supermarkets or high traffic areas, so the network manager of the bank must provide connectivity for a cash machine or branch office with short lead times. Hotels need basic connectivity at new locations to handle reservations and credit card transactions. Delays in circuit installation can mean lost business.

Wireless broadband is also advantageous to an enterprise customer as a backup or alternative means of connectivity. As an example, this chapter describes a configuration using a Cisco 1711 router with three WAN interfaces: DSL, wireless broadband, and Async dial-up. If the DSL circuit fails, the wireless broadband is the preferred path. If both DSL and wireless broadband fail, the router creates an encrypted tunnel using dial backup.

**Disadvantages**

One disadvantage of wireless broadband is the lack of coverage guarantee at all times and all locations within the service area. For example, one location tested by Cisco and described in this chapter was between two antenna towers, with each tower less that two miles from the residence. Signal strength to one of the tower locations was limited by terrain and buildings, and was impaired by foliage for the other.

---

**Note**

The wireless broadband service provider offers the following caveat: “Wireless broadband coverage is impacted by, among other things, terrain, weather, antenna location, system modification, foliage, and man-made structures (such as buildings), and can therefore not be predicted precisely at all times.”

The wireless modem management software has a signal quality and strength scale of 0–4. Signal quality is a more important indicator than signal strength. Using either the built-in antenna or an external reverse polarity Yagi antenna (purchased separately), testing revealed that quality and strength are in the range of 1–2 on a scale of 0–4.

The wireless broadband service tested offered impressive average latency, meeting or exceeding cable or DSL performance. The packet loss rate and jitter are generally much higher. For most data applications, this is not noticeable. In testing, a Linksys web server (camera) is accessed using the wireless broadband service and the images are of acceptable quality.

Packet loss and jitter can impact the quality of VoIP, and the test results indicated that the voice quality ranged from very good to very poor. Test results are provided later in this chapter.

**Topology**

This section describes the following two topologies:

- **Single WAN Interface**
- **Multi-WAN Interface**

The single WAN interface topology uses the wireless broadband as the only WAN interface. The multi-WAN interface uses the wireless broadband network as an alternate path to the primary DSL network. The single WAN configuration is used for VoIP performance testing. The standard Chariot teleworker traffic profile is used. Chariot endpoints are located at the employee residence and Cisco lab. The test results use the Internet and are representative of a typical deployment and configuration.

For the multi-WAN configuration, a Linksys web camera was the client/host used to answer pings and to generate network traffic for testing and demonstration.
Note
The Linksys web camera was not deployed or in use during the VoIP testing.

Single WAN Interface

The single WAN interface topology is shown in Figure 7-1:

**Figure 7-1  Wireless Broadband—Single WAN**

The single WAN topology is used for the VoIP performance testing. Only one IPSec peer is defined in the remote router, and failover and recovery was not a test objective.

Two inside VLANs were defined to implement a physical split tunnel configuration. During the performance testing, no spouse and child traffic was included in the profile.

Multi-WAN Interface

The multi-WAN interface is shown in Figure 7-2:
Failover/Recovery Time

The multi-WAN topology takes advantage of key features of the Cisco 1711 router. The Async interface is configured as dial backup to a head-end Cisco 7200 EZVPN server. The Fast Ethernet 0 interface is configured to obtain an IP address from the wireless broadband modem using DHCP. The crypto map on this interface uses RSA keys and a Public-Key Infrastructure (PKI) and Certificate Authority (CA) for authentication. The primary outside interface is defined as a VLAN (200) to the switch module of the Cisco 1711. This interface connects to a DSL router and uses a static IP address. DHCP cannot be used to obtain addresses for a VLAN interface. Authentication also uses RSA keys and a PKI/CA.

A Linksys web camera is attached to the inside or VLAN 1 interface and is used to verify connectivity and to generate sample network traffic. Both the DSL and wireless broadband links have active IPSec tunnels and can pass traffic. The Service Assurance Agent (SAA) probes are generating ICMP packets periodically through their respective tunnels. The Async interface dials the access server of the ISPs only in the event that both the DSL and wireless broadband links are down.

Failover/Recovery Time

The Cisco IOS Reliable Static Routing Backup Using Object Tracking feature was used to monitor and control the backup interface function. How quickly a secondary or tertiary interface is brought online is a function of the configured “down” value of the track command. In testing, the following parameters were used:

```
track 200 rtr 200
delay down 60 up 5
```

Recovery from a path failure takes at least 60 seconds with these values. They are, however, configurable.

**Note** Enabling debug track can provide a visual indication of the quality of the wireless broadband link. Assuming the delay down is configured at 60 and the frequency of the SAA object is 15 seconds, four consecutive SAA packets must be lost for the tracked route to be removed from the routing table. As
Probes are lost, the debug track provides a log message indicating this. If subsequent probes are lost or are successful, this is also logged by debug track. During periods of high packet loss, the number of logged messages increases accordingly.

**Performance Results**

The wireless broadband service tested is the wireless broadband service in the Research Triangle Park, North Carolina, USA area.

The test locations are Cisco employee residences in the Raleigh-Durham, North Carolina area using the same IPSec equipment and infrastructure supporting teleworkers over cable and DSL.

These tests results are from a Cisco 1711 router deployed at the employee residence. Cable service provider - Cable—Business Class Service 3 Mbps/768 kbps is used as a reference. The uplink (or branch-to-head-end leg) is shaped to 600 kbps.

Also installed is the wireless broadband (Platinum Class) shaped 256 kbps up and unlimited down. The antenna tower is less than two miles from the residence. Two tests were run; a best case and a worst case. The best case uses the external Yagi antenna.

The signal strength is 3 of 4 and the signal quality is 4 of 4, on the 0–4 scale, as displayed by the Mobility Manager software, not the external LEDs.

The worst case used the supplied antenna (sometimes called a “popsicle-stick” antenna) shown on the product literature photo of the modem in Wireless Broadband Modem, page 7-9. In testing, the signal strength with this antenna is 0 to 1 and signal quality is 0 to 2. The modem is inside the residence.

There are two goal lines on the following performance results charts:

- **Lab goal**—Value in lab testing that the performance characteristic should not exceed in a lab environment with no appreciable impact because of WAN. Jitter target is less than 8 ms and the latency target is less than 50 ms. Voice packet loss is to be less than 1/2 of one percent.

- **Internet goal**—Higher than the lab goal values because there is some ISP-associated loss, latency, and jitter. These target values are jitter at less than 20 ms, latency at less than 100 ms, and voice packet loss at less than 1 percent.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ITU value is 150 ms or less. Latency even up to 250 ms can be acceptable. Latency was not an issue in any of these tests.</td>
</tr>
</tbody>
</table>

These tests are conducted at a first adopter stage in the wireless broadband service. There is little or no contention for bandwidth by other subscribers. Results can vary based on a variety of factors, including environmental or terrain interference. The same holds true for the cable tests; results are influenced by contention from other subscribers as well as varying degrees of Internet backbone and enterprise campus traffic.

These test results are intended to represent what a typical user may encounter.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>For best results, an external antenna is recommended.</td>
</tr>
</tbody>
</table>

**Average Jitter Comparison**

The average jitter between cable and wireless broadband is compared in Figure 7-3:
The uplink, or branch-to-head-end jitter values are substantially higher than the baseline using cable. However, the router on the cable connection was using hierarchical class-based weighted fair queuing (CBWFQ) and shaped at 600 kbps on the uplink, and the wireless broadband link is shaped at 256 kbps.

Both the cable and wireless broadband link have no service provider guarantee for uplink speed. The values advertised are for burst or maximum uplink speed. In this environment, both the cable and wireless broadband links are tested with VoIP and also with a TCP-based throughput utility and a shaped value is selected that can be conservatively expected to be available most of the time. The goal is not to overrun a modem or head-end infrastructure and drop packets indiscriminately. Packets should be intelligently queued within a shaped rate by the remote router.

To add to the objective data, actual VoIP calls are placed using the wireless broadband to subjectively verify that the voice quality is good.
Voice Loss

The voice loss is compared between cable and wireless broadband in Figure 7-4:

![Voice Loss Diagram]

The percent of bytes lost for the G.729 voice stream is acceptable for cable and wireless broadband using the Yagi antenna. Voice loss using the supplied antenna exceeds the target threshold. Nine percent loss for voice is excessive. Nine percent loss is high even for data-only applications.

*Note*

Voice codecs can manage single packet loss with concealment algorithms. If consecutive packets are lost, it is noticeable to the listener.
Performance Results

Chapter 7  Small Branch—Wireless Broadband Deployment

Average Latency

The average latency is compared between cable and wireless broadband in Figure 7-5:

Figure 7-5  Latency

![Graph showing latency comparison between cable and wireless broadband](image)

The average latency is very good in all configurations. These values are equivalent to what is typically seen in broadband deployments.

Mission Critical Response Time

The Chariot traffic profile also includes data that is marked with Differentiated Services Code Point (DSCP) value of AF21. While many of the tests include a transactional data class allocated a minimum bandwidth of 22 percent, the wireless broadband tests did not include a separate class. Therefore, these packets are in the class default class. The Yagi and supplied antenna tests report .2 seconds and .5 seconds for mission critical response time. The cable value is .1 second. All are reasonably good values.
Wireless Broadband Hardware Components

This section describes the hardware components of the wireless broadband solution, and includes the following topics:

- Wireless Broadband Modem
- Yagi Antenna and Cables
- Cisco 1711 and Cabling
- Yagi Antenna Aiming
- Mobility Manager

Wireless Broadband Modem

The MT-1000 wireless broadband modem (see Figure 7-6) is tested using the included antenna as well as an external Yagi antenna. The plastic side panel of the MT-100 needed to be removed to securely connect the cables for the external antenna.

![Figure 7-6 MT-1000 Wireless Broadband Modem](image)

Note

The Ethernet interface is a 10/100 interface but was tested with Cisco 1711s and not tested with the Cisco 831. The Cisco 831 Ethernet 1 (outside) interface is a 10 Mbps interface and is not a 100 Mbps FastEthernet interface.

Yagi Antenna and Cables

The information of the external antenna is as follows:

- HyperGain® HG1910Y
  High Performance 1850-1970 MHz 10 dBi Radome Enclosed Yagi Antenna
- Standard Connector—Yagi N-female
- Part Number—HG1910Y-NF
- Wireless LAN Radio Pigtails—RP-MMCX Type to N-female 19 in. (LMR/WBC100 cable) part number CA-PHCABLE2

An N-male to N-male connector is required between the standard Yagi N-female connector and the N-female pigtail cable that attaches to the MT-1000. Cable length depends on the distance between the Yagi antenna and the MT-1000.
Cisco 1711 and Cabling

Figure 7-7 shows the remote Cisco 1711 router with the physical cabling and connections.

The F4 (interface Fa4) switch port is configured as VLAN 200 and is connected to a Cisco 837 DSL router (not shown). The F1 (interface Fa1) switch port is configured as VLAN 1 and is connected to the Linksys Web Camera. The F0 (interface Fa0) port is connected to the wireless broadband modem. The analog phone line is connected to the DSL splitter.

Yagi Antenna Aiming

These instructions on aiming the antenna assume that the consumer or an installer knows the location of the nearest antennas.

Yagi antenna are directional antenna and must be aimed at the radio tower for best signal strength and quality. In testing, a vendor contact provided a map marked with the two nearest tower locations and the residence location.

The map did not contain a reference line for either true or magnetic north. A global positioning system (GPS) receiver and the coordinates for the residence are available. By driving to one of the antenna locations and marking its location, the GOTO function on the GPS is used to determine the degrees azimuth. These two values should have a difference of 180 degrees. A GPS receiver when at rest provides no bearing information, but it does indicate the azimuth you must travel to reach the desired location.

To orient the map, the compass base is aligned between the two known points, and the map and compass are rotated until the index line (which is parallel with the base) is over the desired number of degrees. While the map remains in this position, orient the compass base so that the stationary index line is aligned with north, or 0 degrees, and draw a reference line using the compass base as a straight-edge. This puts a magnetic north reference line on the map assuming the number of degrees between the two known positions can be obtained by a GPS set to magnetic declination. Most GPS units can be set to true north or magnetic north with either auto or manual declination.
With the map remaining facing North, the compass base can be aligned between the Yagi antenna location and the second tower. The number of degrees indicated by the index mark is the azimuth the antenna must face (80 degrees in this test). The azimuth between the residence and the first tower is 301 degrees and from the tower to the house is 121 degrees. These values must be 180 degrees different to be correct.

*Figure 7-8* shows the Yagi antenna pointed approximately 80 degrees to the second tower with the compass and map.

*Figure 7-8  Aiming the Yagi*

Ideally, the Yagi is attached outside the structure. It saves time by first testing on a tripod or temporary support before permanently mounting.

**Mobility Manager**

The wireless broadband service includes Mobility Manager software. This software is installed on a PC, and the PC Ethernet interface and the wireless broadband modem are connected with a straight-through Ethernet CAT5 cable. Signal strength and quality are displayed on their own four-point scale to fine-tune the Yagi antenna.
You can also use the software to upload firmware updates to the modem and to determine its status. You should also use this software to verify the connection before connecting to a router. Because the modem contains its own DHCP server, there is no problem moving the cable between a PC and the router interface configured as a DHCP client. Samples of best and worst case signal strength and quality are shown in Figure 7-9:

**Figure 7-9 Mobility Manager**

For usability with visual and audible confirmation, live voice calls are placed over the wireless broadband link and a Linksys web camera is viewed. The performance charts for the Chariot test scripts are described in the performance section. Figure 7-10 shows a screen print of the image from the camera.
In the multi-WAN configuration, the DSL and wireless broadband links are failed, forcing the Cisco 1711 into a dial-up mode. From a head-end campus, the IP address of the web camera is the target of a ping during the failure scenarios to verify that IKE Keepalive/DPD/RRI is removing routes from the routing table and also from EIGRP advertisements between the three IPSec head-end routers.

Note
The three IPSec head-end routers exchange routes using the 192.168.82.0 network.

Configuration

This section describes the configurations for the various components of the wireless broadband solution, and includes the following topics:

- Multi-WAN Cisco 1711 Router
- Single WAN Remote Router
- EZPVN Head-end Server
- Primary IPSec Head-end
- Secondary IPSec Head-end

Multi-WAN Cisco 1711 Router

The configuration for the multi-WAN Cisco 1711 router is as follows:

```
!!
version 12.3
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service tcp-small-servers
```
hostname vpn-jk2-1711-1
!
boot-start-marker
boot system flash c1700-k9o3sy7-mz.123-2.XF
boot-end-marker
!
logging buffered 2048000 debugging
enable secret 5 $xxxxvvvvvvvvvv
!
username ese_vpn_team privilege 15 secret 5 vvvvvvvvvvvv.
clock timezone est -5
clock summer-time edt recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
!
ip tftp source-interface Vlan1
no ip domain lookup
ip domain name cisco.com
ip host harry 172.26.129.252
ip host rtp5-esevpn-ios-ca 10.81.0.27
ip name-server 207.69.188.185
ip name-server xx.xxx.6.247
ip name-server 171.68.226.120
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip audit notify log
ip audit po max-events 100
ip dhcp-client default-router distance 222
!
track 150 rtr 150
delay down 60 up 5
!
track 200 rtr 200
delay down 60 up 5
no ftp-server write-enable
chat-script MODEM "'atdt'T" TIMEOUT 60 CONNECT \c
!
crypto ca trustpoint rtp5-esevpn-ios-ca
enrollment url http://rtp5-esevpn-ios-ca:80
revocation-check none
source interface Vlan1
auto-enroll 70
!
crypto ca certificate chain rtp5-esevpn-ios-ca
certificate 23
quit
certificate ca 01
quit
!
Refer to status of CSCef87216
crypto isakmp policy 10
crncr 3des
group 2
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
!
crypto ipsec transform-set TUNNEL_3DES_SHA esp-3des esp-sha-hmac
!
!
crypto ipsec client ezvpn RTP5-ESVPN-GW3
  connect auto
  group EZVPN_Group key [must_match_Group_in_Head-end]
  mode network-extension
  peer xx.xxx.223.24
  username vpn-jk2-1711-1 password [must_match_PW_in_Head-end]
  
  crypto map RTP5-ESVPN-GW4 10 ipsec-isakmp
  description IPsec Peer for DSL Link
  set peer xx.xxx.223.24
  set transform-set TUNNEL_3DES_SHA
  match address CRYPTO_MAP_ACL
  qos pre-classify
  
  crypto map RTP5-ESVPN-GW5 10 ipsec-isakmp
  description IPsec Peer for Broadband Wireless
  set peer xx.xxx.223.25
  set transform-set TUNNEL_3DES_SHA
  match address CRYPTO_MAP_ACL
  qos pre-classify

!
!
!
class-map match-all VOICE
  match ip dscp ef

class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3

class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6

match access-group name IKE
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21

  See policy-map BLOCK_VoIP there will be no VoIP on the backup links

policy-map BACKUP-INTERFACES
  class INTERNETWORK-CONTROL
    bandwidth percent 5
    set dscp cs6
  class TRANSACTIONAL-DATA
    bandwidth percent 22
  class class-default
    fair-queue
    random-detect
    
  policy-map Shaper-WIRELESS
  class class-default
    shape average 102400# Interval not set to 10ms as no VoIP on this link.
    fair-queue
    random-detect
    service-policy BACKUP-INTERFACES
  
  policy-map BLOCK_VoIP
description Prevent an IP Phone from registering on this link
   class VOICE
       police 8000 conform-action drop exceed-action drop
   class CALL-SETUP
       police 8000 conform-action drop exceed-action drop
policy-map V3PN-teleworker
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
   class CALL-SETUP
       bandwidth percent 2
   class INTERNETWORK-CONTROL
       bandwidth percent 5
       set dscp cs6
   class VOICE
       priority 128
   class TRANSACTIONAL-DATA
       bandwidth percent 22
   class class-default
       fair-queue
       random-detect
policy-map Shaper-DSL
   class class-default
       shape average 182400 1824
   service-policy V3PN-teleworker
!
!
interface FastEthernet0
description Outside to MT-1000 Wireless Broadband MODEM
   ip dhcp client route track 150
   ip address dhcp
   ip access-group INPUT_ACL in
   service-policy input BLOCK_VoIP
   service-policy output Shaper-WIRELESS
   ip route-cache flow
   load-interval 30
duplex auto
   speed auto
   no cdp enable
crypto map RTPS-ESEVPN-GW5
!
interface FastEthernet1
description Inside to WEB Camera
   no ip address
   vlan-id dot1q 1
   exit-vlan-config
!
interface FastEthernet2
   no ip address
   vlan-id dot1q 1
   exit-vlan-config
!
interface FastEthernet3
   no ip address
   vlan-id dot1q 1
   exit-vlan-config
!
interface FastEthernet4
description Outside to DSL Router
   switchport access vlan 200
   no ip address
!
interface Vlan1
description Inside
ip address 10.81.7.225 255.255.255.248
ip inspect CBAC in
ip route-cache flow
tcp adjust-mss 542
crypto ipsec client ezvpn RTP5-ESEVPN-GW3 inside

interface Vlan200
description Outside to DSL Router
ip address 192.168.2.211 255.255.255.0
ip access-group INPUT_ACL in
service-policy output Shaper-DSL
ip route-cache flow
crypto map RTP5-ESEVPN-GW4

interface Async1
description EarthLink Dialup Service V34/LAPM/V42B/24000:TX/26400:RX
bandwidth 24
ip address negotiated
ip access-group INPUT_ACL in
service-policy input BLOCK_VoIP
service-policy output BACKUP-INTERFACES
encapsulation ppp
ip route-cache flow
load-interval 30
dialer in-band
dialer string 6550070
dialer-group 21
async mode dedicated
ppp authentication pap callin
ppp pap sent-username xxxxxxx@mindspring.com password 7 vvvvvvvvvvvvvvvv

crypto ipsec client ezvpn RTP5-ESEVPN-GW3

ip classless

A default route will be available via DHCP with an administrative distance of 222,
based on the ip dhcp-client default-router distance 222 command.

The DSL router’s IP address is 192.168.2.1

ip route 0.0.0.0 0.0.0.0 192.168.2.1 200 name Quad_Zero_via_DSL track 200
ip route 0.0.0.0 0.0.0.0 Async1 240 name DIAL_BACKUP

The EZVPN IOS Head-end Server is xx.xxx.223.23

ip route xx.xxx.223.23 255.255.255.255 Async1 name DIAL_BACKUP_IPSEC_peer
ip route xx.xxx.223.23 255.255.255.255 Null0 223 name DUMP_when_int_down

The IPSec peer for the DSL link

ip route xx.xxx.223.24 255.255.255.255 Vlan200 192.168.2.1 permanent name DSL_router

The IPSec peer for the Wireless Broadband link

ip route xx.xxx.223.25 255.255.255.255 FastEthernet0 dhcp 222
ip route xx.xxx.223.25 255.255.255.255 Null0 223 name DUMP_when_int_down

ip route 172.30.30.128 255.255.255.255 FastEthernet0 dhcp # Host route to Wirless MODEM

no ip http server
no ip http secure-server
ip flow-export version 5
!
!
ip access-list extended CRYPTO_MAP_ACL
   permit ip 10.81.7.224 0.0.0.7 any
ip access-list extended IKE
   permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
   remark Allow IKE and ESP from the RTP headends
   permit udp xx.xxx.16 0.0.0.15 any eq isakmp
   permit udp xx.xxx.223.16 0.0.0.15 any eq non500-isakmp
   permit esp xx.xxx.223.16 0.0.0.15 any
   remark Cisco Corporate Subnets (not complete)
   permit ip xxxx.44.0.0 0.0.255.255 10.81.7.224 0.0.0.7
   permit ip xxxx.68.0.0 0.3.255.255 10.81.7.224 0.0.0.7
   permit ip xxxx.16.0.0 0.15.255.255 10.81.7.224 0.0.0.7
   permit ip xxxx.168.0.0 0.0.255.255 10.81.7.224 0.0.0.7
   permit ip xxxx.107.0.0 0.0.255.255 10.81.7.224 0.0.0.7
   permit ip xx.100.0.0 0.3.255.255 10.81.7.224 0.0.0.7
   permit ip xx.104.0.0 0.0.255.255 10.81.7.224 0.0.0.7
   permit ip xx.0.0.0 0.255.255.255 10.81.7.224 0.0.0.7
   permit udp any any eq bootpc
   remark NTP ACLs
   permit udp 192.5.41.40 0.0.0.1 eq ntp any
   permit udp host 216.210.169.40 eq ntp any
   remark SSH from RTP Ridge
   permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
   permit icmp any any
   deny ip any any
   access-list 121 remark Define Interesting Traffic
   access-list 121 permit ip any any
dialer-list 21 protocol ip list 121
!
control-plane
!
rtr responder
rtr 12
type echo protocol ipIcmpEcho xxxx.26.129.252 source-ipaddr 10.81.7.225
request-data-size 164
tos 192
frequency 90
lives-of-history-kept 1
buckets-of-history-kept 60
filter-for-history all
rtr schedule 12 life forever start-time now
rtr 150
type echo protocol ipIcmpEcho xx.102.223.25 source-ipaddr 10.81.7.225
tos 192
timeout 500
owner vpn-jk2-1711-1
tag TRACKING_PROBE_FOR_WIRELESS_BROADBAND
frequency 15
lives-of-history-kept 1
buckets-of-history-kept 20
filter-for-history failures
rtr schedule 150 life forever start-time now
!
rtr 200
type echo protocol ipIcmpEcho xx.xxx.223.24 source-ipaddr 10.81.7.225
tos 192
timeout 200
owner vpn-jk2-1711-1
tag TRACKING_PROBE_FOR_DSL
frequency 15
lives-of-history-kept 1
buckets-of-history-kept 20
filter-for-history failures
rtr schedule 200 life forever start-time now
!
alias exec vlandata vlan database
!
line con 0
exec-timeout 60 0
login local
stopbits 1
line 1
script dialer MODEM
modem InOut
modem autoconfigure discovery
transport input all
transport output pad udptn telnet rlogin ssh
stopbits 1
speed 115200
flowcontrol hardware
line aux 0
stopbits 1
line vty 0 4
login local
transport input ssh
!
exception memory minimum 786432
ntp clock-period 17179979
ntp server 192.5.41.41
ntp server 192.5.41.40
ntp server 216.210.169.40
ntp server 10.81.254.202 source Vlan1
end

**Single WAN Remote Router**

This Cisco 1711 router is configured with a “physical” split tunnel. The spouse and child computers are on the VLAN 2 logical interface and their addresses are available via NAT/pNAT to the Internet unencrypted. All corporate traffic is encrypted and sent to the corporate head-end. During performance testing, no spouse and child traffic is present in the Chariot traffic profile.

! version 12.3
no service pad
service timestamps debug datatime msec localtime show-timezone
service timestamps log datatime msec localtime show-timezone
service password-encryption
!
hostname steve-vpn-1711
!
boot-start-marker
boot system flash:c1700-k9o3sy7-mz.123-8.T3.bin
boot-end-marker
!
logging buffered 200000 debugging
!
username ese_vpn_team privilege 15 secret 5 xxxx
clock timezone est -5
clock summer-time edt recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
ip dhcp pool Client  # Corporate Network Address space, not NAT
    network 10.81.7.168 255.255.255.248
    default-router 10.81.7.169
    dns-server xx.xxx.6.247 171.68.226.120
    domain-name cisco.com
    option 150 ip xx.xxx.2.93
    netbios-name-server 171.68.235.228 171.68.235.229
!
ip dhcp pool SpouseChild# Spouse and Child will be NAT/pNAT‘ed
    import all
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
!
ip telnet source-interface Vlan1
ip tftp source-interface Vlan1
no ip domain lookup
ip domain name cisco.com
ip host harry 172.26.129.252
ip host rtp5-esevpn-ios-ca 10.81.0.27
ip name-server 207.69.188.185
ip name-server xx.xxx.6.247
ip cef
ip inspect max-incomplete high 1400
ip inspect one-minute high 1400
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip ips po max-events 100
ip ssh source-interface Vlan1
!
crypto pki trustpoint rtp5-esevpn-ios-ca
    enrollment url http://rtp5-esevpn-ios-ca:80
    revocation-check none
    source interface Vlan1
    auto-enroll 70
!
crypto pki certificate chain rtp5-esevpn-ios-ca
    certificate 16
    certificate ca 01
!
class-map match-all VOICE
    match ip dscp ef
class-map match-any CALL-SETUP
    match ip dscp af31
    match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
    match ip dscp cs6
    match access-group name IKE
!
policy-map V3PN-teleworker
description Note: LLQ for ATM/DSL G.729=64K, G.711=128K

class CALL-SETUP
  bandwidth percent 2
class INTERNETWORK-CONTROL
  bandwidth percent 5
class VOICE
  priority 128
  class class-default
    fair-queue
    random-detect

policy-map Shaper-wireless
  description (real is wireless-Platinum) assume 256kbps up
  class class-default
    shape average 256000 2560 0
  service-policy V3PN-teleworker

  crypto isakmp policy 1
  encr 3des
  group 2
  crypto isakmp keepalive 10

  crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac
  no crypto ipsec nat-transparency udp-encaps

  crypto map RTP 1 ipsec-isakmp
  description RTP Enterprise Class Teleworker
  set peer xx.xxx.223.24
  set peer xx.xxx.221.26# A Second peer could be defined
  set security-association lifetime seconds 14400
  set transform-set REPLAY
  match address CRYPTO_MAP_ACL
  qos pre-classify

  interface FastEthernet0
  description Outside
  bandwidth 256
  ip address dhcp
  ip access-group INPUT_ACL in
  ip access-group INPUT_ACL_out out
  ip nat outside
  ip virtual-reassembly
  service-policy output Shaper-wireless
  load-interval 30
duplex auto
  speed auto
  no cdp enable
  crypto map RTP

  interface FastEthernet1
  description SPOUSECHILD-ONLY-VLAN2-ONLY
  switchport access vlan 2
  no ip address
  load-interval 30

  interface FastEthernet2
  description CORPUSER-ONLY-VLAN1-ONLY
  no ip address
  load-interval 30

  interface FastEthernet3
  description CORPUSER-ONLY-VLAN1-ONLY
  no ip address
  load-interval 30
! interface FastEthernet4
description TO-AP-VLAN1or2 based off of AP login
switchport mode trunk
no ip address
load-interval 30
vlan-range dot1q 1 2
description this port can be VLAN 1 or 2
exit-vlan-config
!
! Inside Interface ip tcp adjust-mss 542 was not defined
!
interface Vlan1
description Inside
ip address 10.81.7.169 255.255.255.248
ip inspect CBAC in
load-interval 30
!
!
! This address space will be NAT/pNAT’ed and is unencrypted to the Internet
!
interface Vlan2
description SpouseChild lanside
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip inspect CBAC in
ip virtual-reassembly
load-interval 30
!
!
interface Async1
no ip address
shutdown
!
ip classless
!
! This address 172.30.30.128 is the DHCP server on the MODEM
!
! ip route 172.30.30.128 255.255.255.255 FastEthernet0 65.76.244.213
!
ip nat inside source list pNAT_ACL interface FastEthernet0 overload
!
!
ip access-list extended CRYPTO_MAP_ACL
permit ip 10.81.7.168 0.0.0.7 any
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp
ip access-list extended INPUT_ACL
remark Allow IKE and ESP from the RTP headends
permit udp xx.xxx.223.16 0.0.0.15 any eq isakmp
permit udp xx.xxx.223.16 0.0.0.15 eq isakmp any
permit esp xx.xxx.223.16 0.0.0.15 any
remark double ACL check not applicable in this IOS version
permit udp any any eq bootpc
remark NTP ACLs
permit udp 192.5.41.40 0.0.0.1 eq ntp any
permit udp host 216.210.169.40 eq ntp any
remark SSH from RTP Ridge
permit tcp xx.xxx.87.0 0.0.0.255 any eq 22
permit icmp any any
deny ip any any
ip access-list extended INPUT_ACL_out
EZVPN Head-end Server

The configuration for the EZVPN head-end server is as follows:

```
! version 12.3
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname rtp5-ezevpn-gw3
!
boot-start-marker
boot system disk0:c7200-ik9o3s-mz.123-4.T3
boot-end-marker
!
logging queue-limit 100
logging buffered 100000 debugging
enable secret 5 xxxx
!
username vpn-jk2-1711-1 secret 5 [must_match_PW_in_remote]
clock timezone est -5
clock summer-time edt recurring
aaa new-model
!
!
aaa authentication login default group tacacs+ enable
aaa authentication login RTP_ezvpn_user local
aaa authentication ppp default if-needed group radius
aaa authorization network RTP_ezvpn_group local
aaa session-id common
ip subnet-zero
!
!
ip cef
ip domain name cisco.com
ip host harry.cisco.com 172.26.129.252
ip host rtp5-ezevpn-ios-ca 10.81.0.27
ip name-server xx.xxx.6.247
!
!
crypto ca trustpoint rtp5-ezevpn-ios-ca
	enrollment url http://rtp5-ezevpn-ios-ca:80
revocation-check crl
auto-enroll 70
!
!
crypto ca certificate chain rtp5-ezevpn-ios-ca
```
certificate 21
certificate ca 01
!
!
crypto isakmp policy 10
en cr 3des
authentication pre-share
group 2
crypto isakmp keepalive 10
crypto isakmp client configuration address-pool local dynpool
crypto isakmp xauth timeout 60
!
crypto isakmp client configuration group EZVPN_Group
  key [must_match_Group_in_remote]
dns xx.xxx.6.247 371.68.226.120
domain cisco.com
pool dynpool
save-password
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto dynamic-map DYNOMAP 10
  set transform-set 3DES_SHA_TUNNEL
  reverse-route
!
!
crypto map EZmap local-address Loopback0
crypto map EZmap client authentication list RTP_ezvpn_user
crypto map EZmap isakmp authorization list RTP_ezvpn_group
crypto map EZmap client configuration address respond
crypto map EZmap 10 ipsec-isakmp dynamic DYNOMAP
!
!
controller ISA 2/1
!
!
interface Loopback0
  description Public address
  ip address xx.xxx.223.23 255.255.255.255
!
interface FastEthernet0/0
  no ip address
  shutdown
duplex half
!
interface FastEthernet1/0
description Private
  ip address 10.81.0.23 255.255.255.240
  ip access-group DoS_Input_Queue_Wedge in
  ip route-cache same-interface
  ip route-cache flow
duplex full
  speed 100
  standby 1 ip 10.81.0.20
  standby 1 priority 90* This router has the least favorable priority.
  standby 1 preempt
  standby 1 authentication eSeVpN
  crypto map EZmap
!
interface FastEthernet1/1
description VLAN 101 RTP5-ALPHA-GW1
ip address 192.168.82.23 255.255.255.0
ip route-cache flow
duplex full
speed 100
!
interface Virtual-Template1
no ip address
ppp authentication chap callin
!
router eigrp 64
redistribute static metric 1000 100 255 1 1500 route-map RRI
network 192.168.82.0
no auto-summary
no eigrp log-neighbor-warnings
!
ip local pool dynpool 10.81.7.241 10.81.7.246
ip classless
ip route 0.0.0.0 0.0.0.0 10.81.0.17
no ip http server
no ip http secure-server
!
!
ip access-list extended DoS_Input_Queue_Wedge
deny 53 any any
deny 55 any any
deny 77 any any
deny pim any any
permit ip any any
ip radius source-interface Loopback0
access-list 1 permit 10.81.0.0 0.0.0.255
access-list 1 deny any
access-list 1 remark Home user address pool(s)
snmp-server location Creeksize RTP building 5
snmp-server contact cisco789@cisco.com 919-123-4567
snmp-server enable traps tty
!
route-map RRI permit 10
description Redistribute remote subnets from RRI
match ip address 1
!
! # some config items removed
!
end

Primary IPSec Head-end

The following is an abbreviated configuration of the primary IPSec head-end router:

version 12.3
!
hostname rtp5-esevpn-gw4
!
boot-start-marker
!
boot-end-marker
!
image file is "flash:c3725-adventerprisek9-mz.123-7.11.T"
!
ip cef
!
crypto pki trustpoint rtp5-esevpn-ios-ca
    enrollment url http://rtp5-esevpn-ios-ca:80
    revocation-check crl
    auto-enroll 70
!
!
crypto pki certificate chain rtp5-esevpn-ios-ca
    certificate 15
    certificate ca 01
!
!
crypto isakmp policy 10
    encr 3des
    group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
    mode transport
!
!
crypto dynamic-map RTP_DYN0 10
    set security-association lifetime seconds 28800
    set transform-set 3DES_SHA_TUNNEL
    reverse-route
    qos pre-classify
!
!
crypto map RTP local-address Loopback0
crypto map RTP 1 ipsec-isakmp dynamic RTP_DYN0
!
interface Loopback0
    description Public address
    ip address xx.xxx.223.24 255.255.255.255
!
interface FastEthernet0/0
    description VLAN 100 RTP5-Alpha-GW1
    ip address 10.81.0.24 255.255.255.240
    ip access-group DoS_Input_Queue_Wedge in
    no ip redirects
    ip route-cache same-interface
    ip route-cache flow
    load-interval 30
    speed 100
    full-duplex
    standby 1 ip 10.81.0.20
    standby 1 priority 110  # This is the highest or most favored of the three
    standby 1 preempt
    standby 1 authentication eSeVpN
crypto map RTP
!
interface FastEthernet0/1
    description VLAN 101 RTP5-Alpha-GW1
    ip address 192.168.82.24 255.255.255.0
    speed 100
    full-duplex
    router eigrp 64
    redistribute static metric 1000 100 255 1 1500 route-map RRI
    network 192.168.82.0
    no auto-summary
no eigrp log-neighbor-warnings
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.81.0.17
ip route 10.81.7.0 255.255.255.0 Null0
access-list 1 permit 10.81.7.0 0.0.0.255
access-list 1 deny any log
!
route-map RRI permit 10
description Redistribute remote subnets from RRI
match ip address 1
!
end

Secondary IPSec Head-end

The following is an abbreviated configuration of the secondary IPSec head-end router:

!
hostname rtp5-esevpn-gw5
!
boot-start-marker
boot system flash c3725-advsecurityk9-mz.123-7.11.T
boot-end-marker
!
ip cef
!
!crypto pki trustpoint rtp5-esevpn-ios-ca
  enrollment url http://rtp5-esevpn-ios-ca:80
  revocation-check crl
  auto-enroll 70
!
!crypto pki certificate chain rtp5-esevpn-ios-ca
  certificate 04
  certificate ca 01
!
!crypto isakmp policy 10
  encr 3des
  group 2
  crypto isakmp keepalive 10
!
!crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
mode transport
!
!crypto dynamic-map RTP_DYNO 10
  set security-association lifetime seconds 28800
  set transform-set 3DES_SHA_TUNNEL
  reverse-route
gos pre-classify
!
!crypto map RTP local-address Loopback0
crypto map RTP 1 ipsec-isakmp dynamic RTP_DYNO
!
interface Loopback0
    description Public address
    ip address \textbf{xx.xxx.223.25} 255.255.255.255
!
interface FastEthernet0/0
    description Private
    ip address 10.81.0.25 255.255.255.240
    ip access-group DoS_Input_Queue_Wedge in
    no ip redirects
    service-policy input INGRESS_Policy
    ip route-cache same-interface
    ip route-cache flow
    load-interval 30
    speed 100
    full-duplex
    standby 1 ip 10.81.0.20
    standby 1 preempt # Default HSRP priority is 100
    standby 1 authentication eSeVpN
    crypto map RTP
!
interface FastEthernet0/1
    description VLAN 101 RTP5-Alpha-GW1
    ip address 192.168.82.25 255.255.255.0
    speed 100
    full-duplex
!
router eigrp 64
    redistribute static metric 1000 100 255 1 1500 route-map RRI
    network 192.168.82.0
    no auto-summary
    no eigrp log-neighbor-warnings
!
    ip classless
    ip route 0.0.0.0 255.255.255.0 Null0
!
access-list 1 permit 10.81.7.0 0.0.0.255
access-list 1 deny any log
!
route-map RRI permit 10
    description Redistribute remote subnets from RRI
    match ip address 1
    match ip address 1
    end

\textbf{Cisco IOS Versions Tested}

The following Cisco IOS versions were used in testing:

- vpn-jk2-1711-1—c1700-k9o3sy7-mz.123-2.XF (see Caveats, page 7-29, regarding CSCef87216 (multi-WAN))
- steve-vpn-1711—c1700-k9o3sy7-mz.123-8.T3 (single WAN)
- DSL router—c837-k9o3sy6-mz.123-4.T3
- rtp5-esevpn-gw3—c7200-ik9o3s-mz.123-4.T3
- rtp5-esevpn-gw4—c3725-adventerprisek9-mz.123-7.11.T
- rtp5-esevpn-gw5—c3725-adventerprisek9-mz.123-7.11.T
Caveats

Cisco no longer supports the use, or need for, LAN Access Mobility (LAM), and it was not used in these configurations and tests with the wireless modem.

This section describes the issues encountered during testing, and includes the following sections:

- EZVPN
- DHCP Server

EZVPN

Initially, Cisco IOS version 12.3(8)T4 was installed on the Cisco 1711 router, but because of a software issue, an IKE policy could not be present in the router configuration if EZVPN was also being used as an authentication method. Cisco IOS version 12.3(2)XF did not exhibit this issue.

DHCP Server

The wireless broadband modem provides a local DHCP server to supply an IP address to the host or router attached. Although the IP address provided for the default gateway and the DHCP client is an Internet routable address, (in this example 65.76.244.214), the IP address of the DHCP server is not. The address of the DHCP server is always 172.30.30.128, as shown in the following display.

```
vpn-jk2-1711-1#show dhcp lease
Temp IP addr: 65.76.244.214 for peer on Interface: FastEthernet0
Temp sub net mask: 255.0.0.0
  DHCP Lease server: 172.30.30.128, state: 3 Bound
  DHCP transaction id: 2324
  Lease: 60 secs, Renewal: 30 secs, Rebind: 52 secs
  Temp default-gateway addr: 65.76.244.213
  Next timer fires after: 00:00:27
  Retry count: 0  Client-ID: cisco-000d.bd64.8aa4-Fa0
  Client-ID hex dump: 636973636F2D303030642E626436342E386161342D466130
  Hostname: vpn-jk2-1711-1

On a multi-WAN configuration, for the router to use the correct interface to reach the DHCP server address, a static host route is required as shown:

```

```
ip route 172.30.30.128 255.255.255.255 FastEthernet0 dhcp
```

```
vpn-jk2-1711-1#show ip route 172.30.30.128
Routing entry for 172.30.30.128/32
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
    * 65.76.244.213
      Route metric is 0, traffic share count is 1

The assigned address has a short lease time of 60 seconds, meaning that the router or PC must request a renewal every 30 seconds, as shown in the following debug.

```
vpn-jk2-1711-1#debug dhcp
DHCP client activity debugging is on
```
Summary

Without the host route to the DHCP lease server, the DHCP request follows the default route to the DSL link. Because the address is an RFC 1918 address, it is not routed over the Internet. The end result is that the DHCP lease is not renewed and the router outside interface flaps continuously.

Summary

Wireless broadband is best suited for its target market of providing mobility to a single PC with either an external or PCMCIA modem. This chapter focused on using an external modem with an attached router. Likely deployment situations are small offices seeking rapid deployment of equipment or multiple WAN interfaces for availability. Voice was also tested to determine the viability of deployments for teleworkers. If sufficient signal strength and quality are available and interference because of environmental or terrain is not an issue, voice quality ranges from good to very good. However, like all wireless media, consistency and availability are often an issue.