# The Tunnel Interface

**April 1994**

**Design Implementation Guide**

## Overview

This document provides information on the tunnel interface in Cisco's Software Release 9.21. It includes some guidelines on the applicability of this new feature and discusses potential drawbacks.

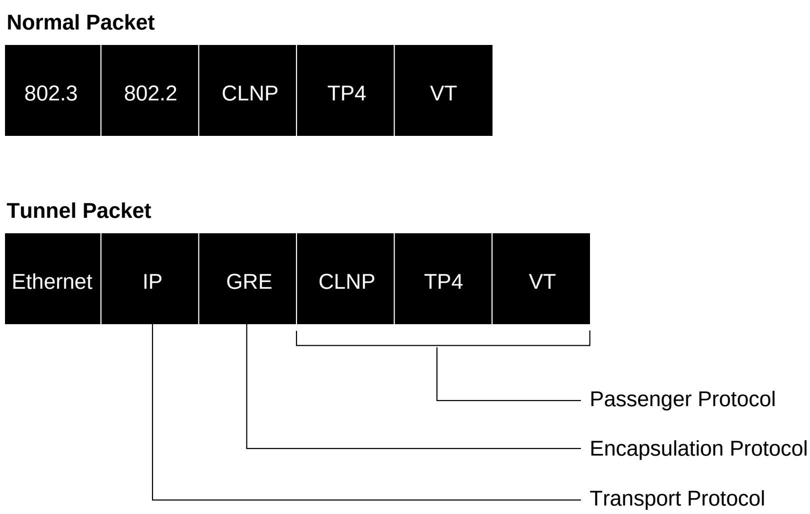
## What Is the Tunnel Interface?

Tunneling provides a way of encapsulating arbitrary packets inside a transport protocol.The tunnel interface is not tied to a particular transport protocol or passenger protocol; it is an architecture designed to provide the services for a point-to-point encapsulation scheme.With tunneling, a virtual interface is implemented that has the look and feel of a physical interface to ease configuration and management.

## Functionality and Terminology

The diagram below compares tunnel packets with "normal" packets and illustrates IP tunneling terminology and concepts. Explanations of the three protocol types used follow the diagram.

**Figure 1. IP Tunneling Terminology and Concepts**




**Passenger Protocol**—the protocol being encapsulated. Cisco currently supports the following:

- IP
- CLNP
- IPX
- Appletalk

**Carrier Protocol—**the encapsulation protocol that provides carrier services. Cisco has implemented the following carrier protocols:

- GRE (Generic Routing Encapsulation), Cisco's multiprotocol carrier protocol
- Cayman, a proprietary protocol for encapsulating Appletalk over IP
- EON (Experimental OSI Network), a standard for carrying CLNP over IP
- NOS IP over IP (compatible with KA9Q)

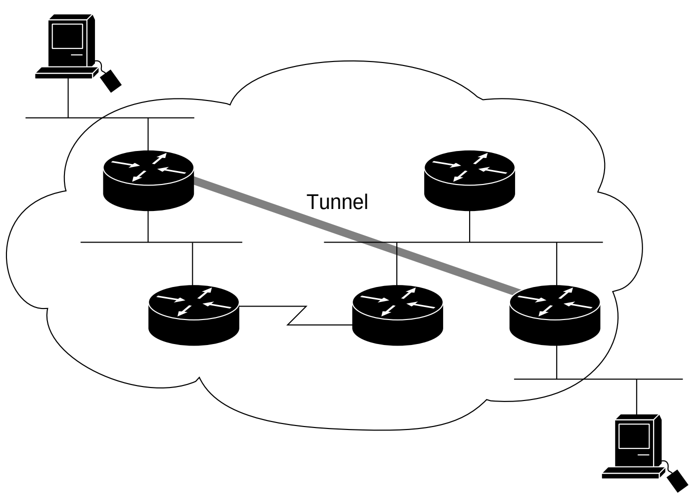
**Transport Protocol—**the protocol used for carrying the encapsulated protocol. Cisco has initially implemented IP; however, the architecture does not preclude other transports protocols from being implemented.

# Reasons for Tunneling

There are multiple situations where tunneling can be of benefit:

- To maintain a single protocol backbone (this should be easier to manage, because backbone routers might be able to switch IP faster than the passenger protocol)
- To serve as a workaround for the hop count constraints of some protocols (see Figure 2).

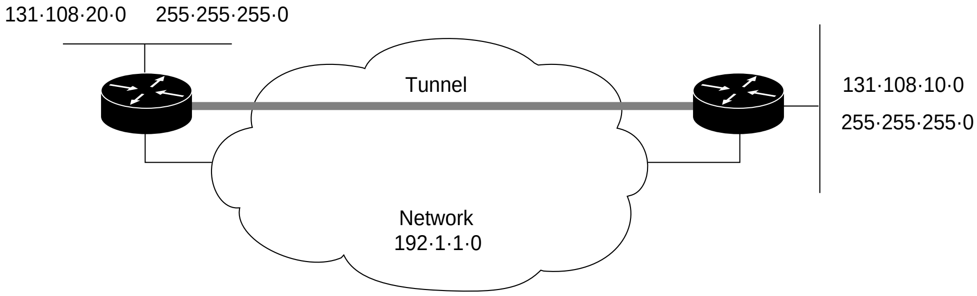
**Figure 2. Workarounds for Networks with Hop Count Limits**




If the path between two computers has more than 15 hops, they cannot talk to each other, If the path between these two computers was greater than 15 hops, they would not be able to communicate. By setting up a tunnel it is possible to hide the underlying physical network.

- To connect discontiguous subnets (see Figure 3).

**Figure 3. Discontiguous Subnetworks**




It is possible for the two subnets of network 131.108.0.0 to talk to each other even though they are separated by another network.

- To build virtual private networks across a WAN

# How It Works

The tunnel interface appears to the passenger protocol to be just like a standard interface. It most closely resembles a point-to-point serial link. The tunneling process works by what could be called a “recursive route lookup.” For example, if IPX is being tunneled, the following steps occur:

1. The destination address of the arriving frame is looked up in the IPX routing table.
2. The IPX routing table points to the tunnel interface.
3. The packet is enqueued on the tunnel interface’s output queue.
4. Instead of a link-level encapsulation, the packet gets a “carrier” header and is passed to the transport protocol (currently only IP is supported).
5. The transport protocol looks up the “tunnel destination address” (hence the recursive route lookup) and enqueues the packet to a real interface.

# Configuration

The configuration commands used are covered in the *Router Products Configuration Guide*, Chapter 6, in the sections entitled “Understand Tunneling” and “Configure IP Tunneling” (pages 25 through 30).

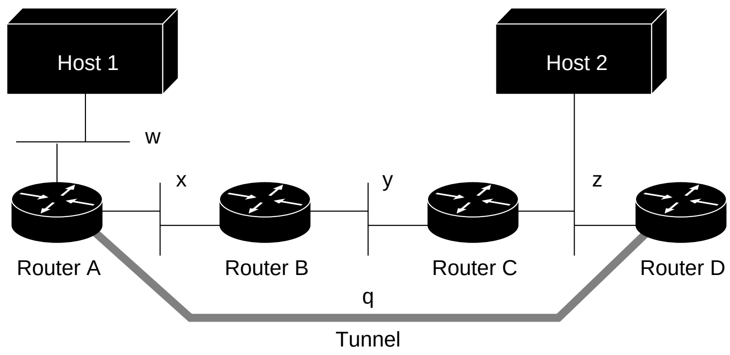
# Caveats

There are many ways to misconfigure tunneling so that you have a completely broken or inefficient topology. Some points to keep in mind are the following:

## Hop Count Limitation

Tunnels look like one-hop, point-to-point links. Routing protocols that make decisions based only on hop count will often prefer a tunnel over a real interface. For example, in Figure 4, packets from host 1 to host 2 will take the path w-q-z rather than the “longer” path of w-x-y-z. In reality, however, the packet will go to router A, get tunneled in IP through networks x, y, and z, get picked up by router D, de-encapsulated, and sent back out onto network z to host 2. Obviously this requires many more steps and more overhead.

**Figure 4. Hop Count Precautions**




## Media Differences

An IP "cloud" can be made up of several different media (an extreme example would be Ethernet and 9.6K lines). Tunneling protocols over this "cloud" (transport protocol network) can wreak havoc with passenger protocols that are not designed to handle delay or dropped frames very well.

## Physical Limitations

It is possible to configure an almost unlimited number of tunnel interfaces, thus alleviating the need to *buy* real interfaces. This might seem like a tempting way of expanding the network, but of course nothing comes for free; several tunnel interfaces through a single physical link can saturate that link. It is also difficult to debug if problems occur in a network with many tunnels heading in all directions.

## Security

Tunnels can allow you to bypass security firewalls by having source and destination addresses that are not covered by access lists in the firewall router.

## Recursive Routing Loops

One of the worst problems that can happen in tunneling is a recursive routing loop. It is important to remember that this problem can *only* occur when the passenger protocol and the transport protocol are the same. Currently, this can *only* happen if tunneling IP, since IP is the only transport protocol supported. In this situation, the best path to the "tunnel destination" is via the tunnel interface. The following steps occur:

**1** The packet is enqueued on the output queue of the tunnel interface.

**2** The tunnel interface puts on a GRE header and enqueues the packet to the transport protocol destined to the destination address of the tunnel interface.

**3** IP looks up the route to the destination address and learns that it is via the tunnel interface.

**4** This returns you to step 1; hence, you are in a recursive routing loop.

**5** To handle this situation, the system shuts down the tunnel interface for 1 to 2 minutes and issues a warning message before it goes into the recursive loop. This causes a lot of route flapping and is an undesirable situation to be in. Another indicator that a recursive route loop has been detected is if the tunnel interface is up and the line protocol is down. To avoid this problem, we recommend always keeping passenger and transport routing information separate. Suggestions for doing so include the following:

- — Use separate AS numbers (for RIP).
- — Use different routing protocols.
- — Give the tunnel interface a very low bandwidth so that routing protocols that can take this into account (such as IGRP) will always have a very high metric for the tunnel interface and will choose the correct next hop (i.e., the *real* interface).

— Keep the two IP address spaces distinct (i.e., use a different major address for your tunnel network and your “real” IP network). This will also be an aid in debugging, because it will be immediately obvious whether an address refers to the tunnel network or the real network.

## Scalability

The most important thing to remember is that tunneled traffic is process switched at only *half* the normal process switching rates. This means approximately 800 pps aggregate for each router. Tunneling is very CPU intensive, and as such, should be turned on cautiously. It is easy to saturate a physical link with routing information if several tunnels are configured over it. There is a system-imposed limit of a maximum of 255 tunnel interfaces in one box; however, nowhere near this number of tunnel interfaces have been successfully configured. Performance will depend on such parameters as the characteristics of the passenger protocol, broadcasts, routing updates, and the bandwidth of physical interfaces.

## References


- Draft RFC: draft-hanks-gre-00.txt
- Draft RFC: draft-hanks-ip-gre-00.txt
- Cisco Systems *Router Products Configuration Guide*
- Software Release 9.21 training course





**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

**European Headquarters**
Cisco Systems Europe s.a.r.l.
Z.A. de Courtaboeuf
16 avenue du Quebec
91961 Les Ulis Cedex
France
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

**Austria**
Cisco Systems Austria
GmbH?World Trade Center
A-1300 Vienna Airport
Austria
Tel: 43 1 71110 6233
Fax: 43 1 71110 6017

**Belgium**
Cisco Systems Bruxelles
Complex Antares
71 avenue des Pleiades
1200 Brussels
Belgium
Tel: 32 2 778 42 00
Fax: 32 2 778 43 00

**Denmark**
Cisco Systems
Larsbjoernsstraede 3
1454 Copenhagen K
Denmark
Tel: 45 33 37 71 57
Fax: 45 33 37 71 53

**Germany**
Cisco Systems GmbH
Max-Planck-Strasse 7
85716 Unterschleissheim
Germany
Tel: 49 89 32 15070
Fax: 49 89 32 150710

**Italy**
Cisco Systems Italy
Via Turati 28
20121 Milan
Italy
Tel: 39 2 62 726 43
Fax: 39 2 62 729 13

**The Netherlands**
Cisco Systems
Stephensonweg 8
4207 HB Gorinchem
The Netherlands
Tel: 31 18 30 22988
Fax: 31 18 30 22404

**Norway**
Cisco Systems
Holmens Gate 4
0250 Oslo
Norway
Tel: 47 22 83 06 31
Fax: 47 22 83 22 12

**South Africa**
Cisco Systems South Africa
Prestige Business Center
Sloane Park 90 Grayston Drive
2152 Sandton
South Africa
Tel: 27 11 784 0414
Fax: 27 11 784 0519

**Spain**
Cisco Systems Spain
Paseo de la Castellana, 141, pl
18
28046 Madrid
Spain
Tel: 34 1 57 203 60
Fax: 34 1 57 045 99

**Sweden**
Cisco Systems AB
Arstaangsvagen 13
11760 Stockholm
Sweden
Tel: 46 8 681 41 60
Fax: 46 8 19 04 24

**Switzerland**
Cisco Systems Switzerland
Grossrietstrasse 7
CH-8606 Naenikon/ZH
Switzerland
Tel: 41 1 905 20 50
Fax: 41 1 941 50 60

**United Arab Emirates**
Cisco Systems (Middle East)
Dubai World Trade Center,
Level-7
P.O. Box 9204
Dubai, U.A.E.
Tel: 971 4 313712
Fax: 971 4 313493

**United Kingdom**
Cisco Systems Ltd.
4 New Square
Bedfont Lakes
Feltham, Middlesex TW14 8HA
United Kingdom
Tel: 44 81 818 1400
Fax: 44 81 893 2824

**Latin American Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
Tel: 408 526-7660
Fax: 408 526-4646

**Asia**
Cisco Systems (HK) Ltd
Suite 1009, Great Eagle Centre
23 Harbour Road
Wanchai, Hong Kong
Tel: 852 2583 9110
Fax: 852 2824 9528

Cisco Systems (HK) Ltd
Beijing Office
Room 821/822, Jing Guang
Centre
Hu Jia Lou, Chao Yang Qu
Beijing 100020 P.R.C.
Tel: 86 1 501 8888 x821
Fax: 86 1 501 4531

Cisco Systems (HK) Ltd
New Delhi Liaison Office
Suite 119, Hyatt Regency Delhi
Bhikaiji Cama Place
Ring Road
New Delhi 110066, India
Tel: 91 11 688 1234
Fax: 91 11 688 6833

Cisco Systems Korea
27th Fl., Korea World Trade
Center
159, Samsung-dong,
Kangnam-ku
Seoul, 135-729, Korea
Tel: 82 2 551 2730
Fax: 82 2 551 2720

Cisco Systems (HK) Ltd
Kuala Lumpur Office
Level 5, Wisma Goldhill
67 Jalan Raja Chulan
50200 Kuala Lumpur, Malaysia
Tel: 60 3 202 1122
Fax: 60 3 202 1822

Cisco Systems (HK) Ltd
Singapore Office
Shell Tower, Level 37
50 Raffles Place
Singapore 0104
Tel: 65 320 8398
Fax: 65 320 8307

Cisco Systems (HK) Ltd
Taipei Office
4F, 25 Tunhua South Road,
Section 1
Taipei, Taiwan
Tel: 886 2 577 4352
Fax: 886 2 577 0248

Cisco Systems (HK) Ltd
Bangkok Office
23rd Floor, CP Tower
313 Silom Road
Bangkok 10500, Thailand
Tel: 66 2 231-0600
Fax: 66 2 231-0448

**Argentina**
Cisco Systems Argentina
Av. del Libertador 602 Piso 5
(1001) Capital Federal
Buenos Aires, Argentina
Tel: 54 1 814 1391
Fax: 54 1 814 1846

**Australia**
Cisco Systems Australia Pty Ltd
Level 17
99 Walker Street
PO Box 469
North Sydney NSW 2060
Australia
Tel: 61 2 935 4100
Fax: 61 2 957 4077

**Brazil**
Cisco Systems Do Brasil
Rua Helena 218, 10th Floor
Cj 1004-1005
Vila Olimpia - CEP 04552-050
Sao Paulo - SP Brazil
Tel: 55 11 822-5413
Tel/Fax: 55 11 853-3104

**Mexico**
Cisco Systems de México, S.A.
de C.V.
Ave. Ejecito Nacional No. 926
3er Piso
Col. Polanco C.P. 11560
Mexico D.F.
Tel: 525 328-7600
Fax: 525 328-7699

**New Zealand**
Cisco Systems New Zealand
Level 16, ASB Bank Centre
135 Albert Street
P.O. Box 6624
Auckland, New Zealand
Tel: 64 9 358 3776
Fax: 64 9 358 4442

**Japanese Headquarters**
Nihon Cisco Systems K.K.
Seito Kaikan 4F
5, Sanbancho, Chiyoda-ku
Tokyo 102, Japan
Tel: 81 3 5211 2800
Fax: 81 3 5211 2810

**Canada**
Cisco Systems Canada Limited
150 King Street West
Suite 1707
Toronto, Ontario M5H 1J9
Canada
Tel: 416 217-8000
Fax: 416 217-8099

**United States**
Central Operations
5800 Lombardo Center
Suite 160
Cleveland, OH 44131
Tel: 216 520-1720
Fax: 216 328-2102

Eastern Operations
1160 West Swedesford Road
Suite 100
Berwyn, PA 19312
Tel: 610 695-6000
Fax: 610 695-6006

Federal Operations
1875 Campus Commons Drive
Suite 305
Reston, VA 22091
Tel: 703 715-4000
Fax: 703 715-4004

Northeastern Operations
One Penn Plaza
Suite 3501
New York, NY 10119
Tel: 212 330-8500
Fax: 212 330-8505

Northern Operations
8009 34th Avenue South
Suite 1452
Bloomington, MN 55425
Tel: 612 851-8300
Fax: 612 851-8311

Service Provider Operations
(Telecommunications)
111 Deerwood Road
Suite 200
San Ramon, CA 94583
Tel: 510 855-4800
Fax: 510 855-4899

Southwestern Operations
14160 Dallas Parkway
Suite 400
Dallas, TX 75248
Tel: 214 774-3300
Fax: 214 774-3333

Western Operations
2755 Campus Drive
Suite 205
San Mateo, CA 94403
Tel: 415 377 5600
Fax: 415 377 5699

Cisco Systems has over
100 sales offices worldwide.
Call the company's corporate
headquarters (California, USA)
at 408 526-4000 to contact your
local account representative or,
in North America, call
800 553-NETS (6387).



L#70901 4/94