

Cisco Virtual Office: DMVPN for IPv6

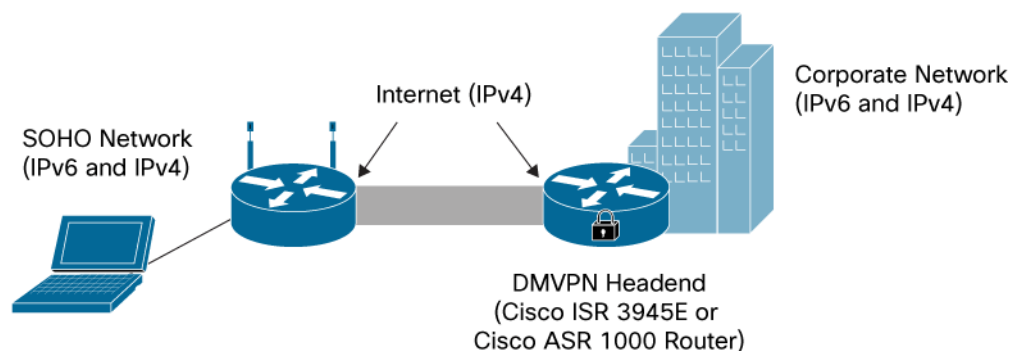
This guide provides detailed design and implementation information relating to the deployment of Dynamic Multipoint VPN (DMVPN) for IPv6 with the Cisco® Virtual Office solution.

Please refer to the Cisco Virtual Office overview (<http://www.cisco.com/go/cvo>) for further information about the solution, its architecture, and all of its components.

Introduction

The Cisco Virtual Office solution includes a DMVPN architecture for data gateway infrastructure. IPv6 is supported on the LAN side of the infrastructure while using the existing IPv4 connectivity for the WAN side. This setup allows enterprises to convert their internal networks to IPv6 while using the existing IPv4 Internet and WAN infrastructure to connect to other sites that are not yet IPv6-compatible. Figure 1 shows the network topology of DMVPN for IPv6.

Figure 1. DMVPN for IPv6 Network Topology



In Figure 1, the small office or home office (SOHO) network behind the spoke router and the corporate network behind the DMVPN hub router can have either IPv6 or IPv4 devices. However, the Internet connection between spoke and hub must be an IPv4 connection.

This guide assumes basic knowledge about DMVPN for IPv4 deployment and basic IPv6 addressing.

Recommended Platforms and Images

The configuration example in this guide uses a Cisco 3945E Integrated Services Router as hub and a Cisco 881W Integrated Services Router as spoke. For other Cisco router platforms, the sample configuration may differ. For a full list of supported hardware and software, please refer to the “Cisco Virtual Office Supported Hardware and Software” guide at <http://www.cisco.com/go/cvo>.

Benefits of Using IPv6

The major advantage of IPv6 over IPv4 is the larger address space. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, or approximately 3.4×10^{38} addressable nodes, providing more than enough globally unique IP addresses for every network device on the planet. As more and more mobile

devices are added to the SOHO network, the need for individual IP addresses is increasing. IPv6 allows the growth of IP networking to continue.

Other benefits of using IPv6 include:

- Better network layer security is ensured by mandatory IP Security (IPsec) integration in IPv6 (optional in IPv4).
- Simpler header compared to IPv4 improves routing efficiency, performance, and forwarding-rate scalability.

Migration Steps (IPv4 to IPv6)

The following describes how to migrate from a DMVPN IPv4 deployment to a DMVPN IPv6 deployment:

- Enable IPv6 in the upstream corporate network for the DMVPN hub routers. In particular, a Domain Name System (DNS) server to manage IPv6 addresses is required.
- Upgrade the hub-and-spoke routers to Cisco IOS® Software Release 12.4(20)T or later.
- Apply DMVPN for IPv6 configurations on hub-and-spoke routers.
- Enable IPv6 on host devices behind the spoke routers.

Deployment Considerations

Things to consider before starting the deployment of DMVPN for IPv6:

- The WAN connection between the hub-and-spoke routers is IPv4 only. Routers in between do not need IPv6 capability.
- Because most websites and DNS servers continue to use IPv4 addresses, it is mandatory to have IPv4 and IPv6 addresses on the host devices behind the spoke router for connectivity to all websites.
- For the LAN side, use IPv6 stateless autoconfiguration (RFC 2462), which requires a 64-bit network prefix. Use stateless autoconfiguration on all devices behind the hub-and-spoke router to avoid manual assignment of IPv6 addresses and to allow easy transition from IPv4 to IPv6.
- IPv6 is supported on Bridge Group Virtual Interface (BVI) only on a Cisco IOS Software 15.1(2)T1 or later image.

Configuring DMVPN for IPv6

The following explains how to configure DMVPN hub-and-spoke routers for IPv6. It covers only the necessary configuration for enabling DMVPN and IPv6. This configuration is only a sample one; it needs to be customized to your correct corporate subnets and servers.

```
Hub-side LAN (corporate) subnet: 10.1.0.0/16
Spoke-side LAN subnet: 10.10.0.0/20 and 10.20.0.0/20
DMVPN tunnel subnet: 192.168.0.0/24
Hub NBMA address: 172.16.0.100
Corporate upstream v6 prefix: 2001:db8:1111::/64
Spoke-side LAN v6 prefix: 2001:db8:BBBB::/48 and 2001:db8:CCCC::/48
DMVPN v6 tunnel prefix: 2001:db8:AAAA::/64
```

Sample DMVPN Hub Configuration for IPv6

```

!!! Hostname and domain name form a fully qualified domain name in certificates
!!!
hostname dmvpn-hub
ip domain-name cisco.com
!
!!! Make sure clock and timezone are in sync !!!
clock timezone PST -8
clock summer-time PDT recurring
ntp server 10.1.1.101
!
!!! Public Key Infrastructure (PKI) configuration !!!
ip host cvo-pki-cs 10.1.1.105
!
crypto pki trustpoint cvo-pki-cs
  enrollment url http://cvo-pki-cs:80
  serial-number
  revocation-check none
  auto-enroll 75
!
!!! Enable IPv6 unicast routing !!!
ipv6 unicast-routing
!
!!! The following routing protocols are supported: Border Gateway Protocol (BGP),
Enhanced Interior Gateway Routing Protocol (EIGRP), On-Demand Routing (ODR), Open
Shortest Path First (OSPF), and Routing Information Protocol (RIP) !!!
ipv6 router eigrp 6
  no shutdown
!
router eigrp 7
  network 10.1.0.0 0.0.255.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
!
!!! IKE/IPSec Configuration !!!
crypto isakmp policy 1
  encr 3des
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
  mode transport
crypto ipsec profile cvo-profile-1
  set transform-set t1
!
!!! Enable IPv6 on upstream interface (connecting to corporate network) !!!
interface GigabitEthernet0/1
  description dmvpn-hub to upstream gateway
  ip address 10.1.2.2 255.255.255.252
  !!! Configure IPv6 address using EUI-64 !!!
  ipv6 address 2001:db8:1111::/64 eui-64

```

```

!!! Auto-generate a link-local address !!!
ipv6 enable
!!! Enable EIGRP on the interface !!!
ipv6 eigrp 6
!
!!! Loopback used as NBMA address !!!
interface Loopback0
  ip address 172.16.0.100 255.255.255.255
!
!!! Tunnel Configuration !!!
interface Tunnel0
  description DMVPN IPv6 Phase 3
  bandwidth 2000
  ip address 192.168.0.1 255.255.255.0
  no ip redirect
  ip mtu 1400
  ip nhrp map multicast dynamic
  ip nhrp network-id 6000
  ip nhrp redirect
  ip tcp adjust-mss 1360
  !!! EIGRP 7 is the IPv4 EIGRP !!!
  no ip split-horizon eigrp 7
  ip summary-address eigrp 7 10.10.0.0 255.255.240.0 5
  ip summary-address eigrp 7 10.20.0.0 255.255.240.0 5
  delay 2000
!!! Every IPv6 NHRP interface is configured with one IPv6 unicast address. This
address can be a globally reachable or unique local address. A static IPv6
address is configured here !!!
ipv6 address 2001:db8:AAAA::1/64
ipv6 enable
ipv6 mtu 1400
ipv6 eigrp 6
!!! Summary address used in DMVPN Phase 3 !!!
no ipv6 split-horizon eigrp 6
ipv6 summary-address eigrp 6 2001:db8:BBBB::/48 5
ipv6 summary-address eigrp 6 2001:db8:CCCC::/48 5
ipv6 nhrp map multicast dynamic
ipv6 nhrp network-id 6000
ipv6 nhrp redirect
  qos pre-classify
  tunnel source Loopback0
  tunnel mode gre multipoint
  tunnel key 600
  tunnel protection ipsec profile cvo-profile-1
!

```

Sample DMVPN Spoke Configuration for IPv6

```
ip hostname dmvpn-spoke
ip domain-name cisco.com
!
clock timezone PST -8
clock summer-time PDT recurring
ntp server 10.1.1.101
!
ip host cvo-pki-cs 10.1.1.105
!
crypto pki trustpoint cvo-pki-cs
  enrollment url http://cvo-pki-cs:80
  serial-number
  revocation-check crl
  source interface Vlan1
  auto-enroll 60
!
!!! Enable IPv6 unicast routing !!!
ipv6 unicast-routing
!
ipv6 router eigrp 6
  no shutdown
!
router eigrp 7
  network 192.168.0.0 0.0.0.255
  network 10.10.0.0 0.0.0.15
  no auto-summary
!
crypto isakmp policy 1
  encr 3des
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
  mode transport
crypto ipsec profile cvo-profile-1
  set transform-set t1
!
!!! Outside Interface is IPv4 only !!!
interface FastEthernet4
  description WAN interface
  ip address dhcp
!
!!! Enable IPv6 on LAN side !!!
interface Vlan10
  description LAN interface
  ip address 10.10.0.1 255.255.255.240
```

```
!!! Statically assigned IPv6 address (EUI-64 can be used instead). Note: A 64-bit
prefix is used to allow stateless autoconfiguration !!!
ipv6 address 2001:db8:BBBB:1::1/64
ipv6 enable
ipv6 eigrp 6
!
!!! Tunnel Configuration !!!
interface Tunnel0
  description DMVPN IPv6 Phase 3
  bandwidth 2000
  ip address 192.168.0.2 255.255.255.0
  no ip redirect
  ip mtu 1400
  ip nhrp map multicast 172.16.0.100
  ip nhrp map 192.168.0.1 172.16.0.100
  ip nhrp network-id 6000
  ip nhrp nhs 192.168.0.1
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  delay 2000
  !!! Tunnel IPv6 unicast address !!!
  ipv6 address 2001:db8:AAAA::2/64
  ipv6 enable
  ipv6 mtu 1400
  ipv6 eigrp 6
  !!! The NBMA address is IPv4 only !!!
  ipv6 nhrp map multicast 172.16.0.100
  ipv6 nhrp map 2001:db8:AAAA::1/64 172.16.0.100
  ipv6 nhrp network-id 6000
  ipv6 nhrp nhs 2001:db8:AAAA::1
  ipv6 nhrp shortcut
  ipv6 nhrp redirect
  qos pre-classify
  tunnel source FastEthernet4
  tunnel mode gre multipoint
```

```
tunnel key 600
tunnel protection ipsec profile cvo-profile-1
!
```

Wireless IPv6 Access

If an integrated wireless access point (AP) is available in the spoke router, IPv6 access can be provided to the wireless hosts.

In case of integrated AP, e.g., those in Cisco 871W or Cisco 1811W routers, IPv6 addresses should be assigned to the virtual bridging interface (BVI). IPv6 addresses on BVI is supported using image 15.1(2)T1 or later.

In case of integrated AP module, e.g., those in Cisco 881W or Cisco 891W routers, you do not need to assign IPv6 address to the AP. By default, the AP allows IPv6 pass-through, and IPv6 traffic is directly routed from the hosts to the router through the AP transparently.

Verification and Troubleshooting

For DMVPN, the following commands are used to verify and monitor the connection and configuration:

- show dmvpn—Displays DMVPN-specific session information
- show ipv6 nhrp—Displays Next Hop Resolution Protocol (NHRP) mapping information
- show ipv6 nhrp multicast—Displays NHRP multicast mapping information
- show ipv6 nhrp summary—Displays NHRP mapping summary information
- show ipv6 nhrp traffic—Displays NHRP traffic statistics information
- clear dmvpn session—Clears DMVPN sessions
- clear ipv6 nhrp—Clears all dynamic entries from the NHRP cache
- debug dmvpn—Displays debug DMVPN session information
- debug nhrp ipv6—Enables NHRP debugging
- debug nhrp condition—Enables NHRP conditional debugging
- debug ipv6 nhrp error—Displays NHRP error-level debugging information

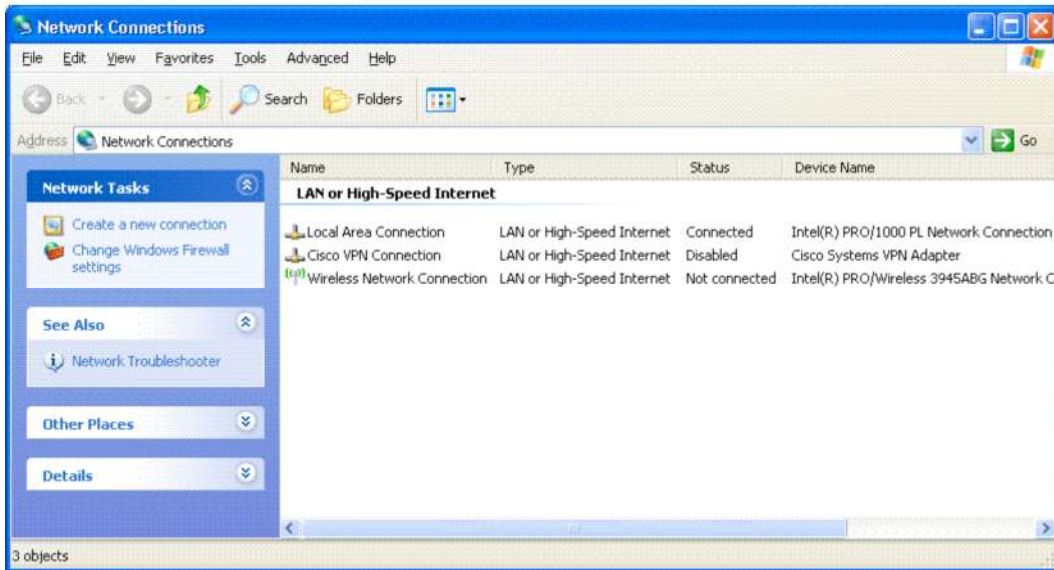
References

- Cisco Virtual Office solution guides and information: <http://www.cisco.com/go/cvo>
- Cisco Feature Navigator: <http://www.cisco.com/go/fn>
- DMVPN: <http://www.cisco.com/go/dmvpn>
- Cisco IPv6: <http://www.cisco.com/ipv6>
- Implementing DMVPN for IPv6: <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ipv6-dmvpn.html>
- Cisco Integrated Services Routers: <http://www.cisco.com/go/isr>
- Cisco IOS Software documentation page: <http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm>
- IPv6 for Microsoft Windows FAQ: <http://www.microsoft.com/technet/network/ipv6/ipv6faq.mspix>

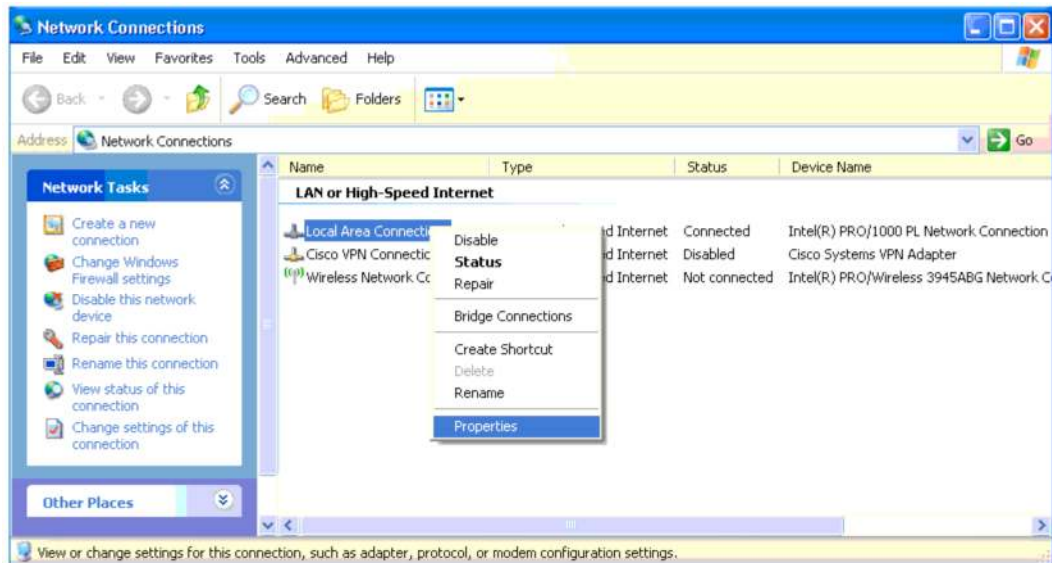
Appendix A

This appendix describes how to install IPv6 for Windows XP. IPv6 is enabled by default on Windows Vista and Windows 7.

1. Click Start, click Control Panel, and then double-click Network Connections.

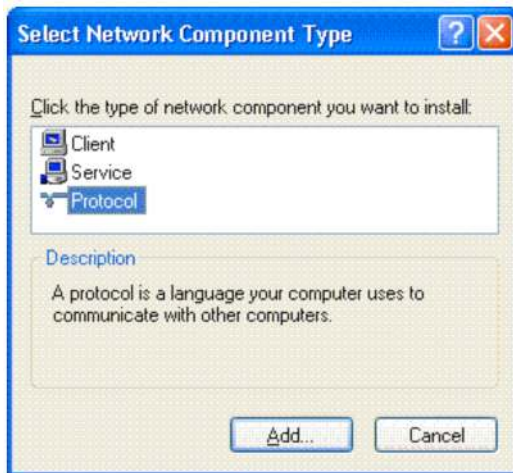


2. Right-click any local area connection, and then click Properties.

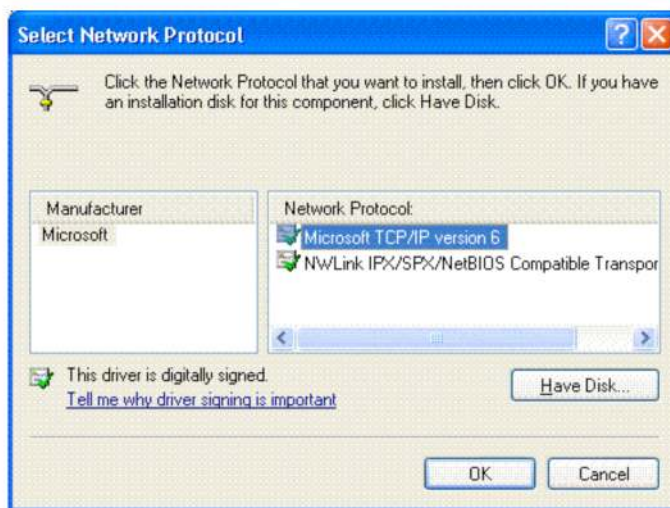


3. Click Install.

4. In the Select Network Component Type dialog box, click Protocol, and then click Add.



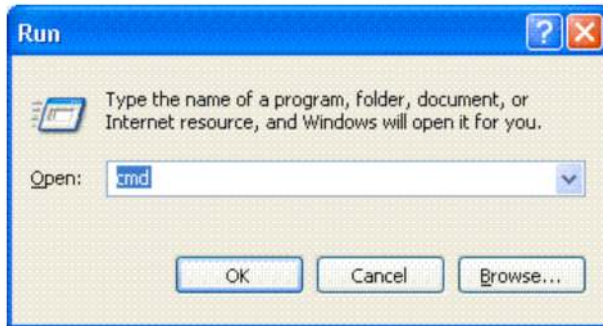
5. In the Select Network Protocol dialog box, click Microsoft TCP/IP version 6 (for SP2 or later)/Microsoft IPv6 Developer Edition (for SP1), and then click OK.



6. Click Close to save changes to your network connection.

Alternatively, you can install IPv6 from the Command Prompt.

1. Click Start, click Run..., type cmd, and then click OK.



2. For Windows XP with SP1 or later, type netsh interface ipv6 install; for Windows XP with no service packs installed, type ipv6 install.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)