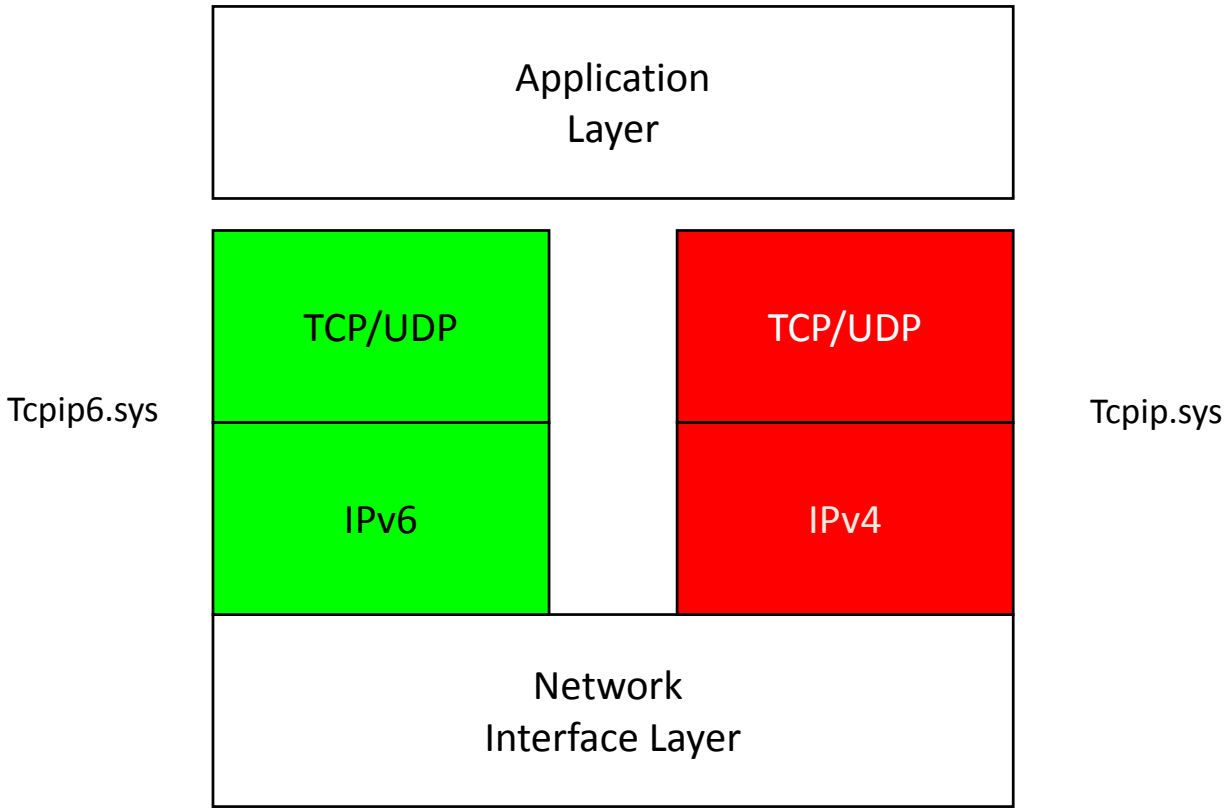
IPv6 en Windows

Ignacio Cattivelli

Juan Jackson

Pablo García

Dual Stack Architecture



- In Windows XP and Windows Server 2003
- Netsh int ipv6 [install|uninstall]

Windows XP SP2 IPv6 Capabilities

- Limited Support:
  - Not on by default, must enable IPv6: netsh int ipv6 install
  - Basic native IPv6 capability, ISATAP, 6to4, Teredo
  - Autoconfiguration & well-known DNS IPs (FEC0)
  - Netsh int ipv6 commands required for config
  - ipconfig, route, ping and ping6, tracert, pathping, netstat
  - IE 6.0, IE7.0, telnet client, ftp clients
  - Filesharing via WebDAV only (e.g. over HTTP)
- Not supported:
  - DHCPv6 client, PPPv6 client
  - AD client protocols (RPC, LDAP, Kerb)
  - File sharing using IPv6 (SMB, NetBT)
  - IPHLPRAPI IPv6, e.g. can't add IPv6 routes via API

Windows Server 2003 SP2 IPv6 Capabilities

- Limited Support:
  - Windows XP SP2 IPv6 functionality, but also…
  - SMB client and server using native IPv6
    - Client won't ping dest first with IPv6 enabled
  - Telnet Server
  - RPC, Simple TCP/IP Services
- Not supported
  - Active Directory Protocols: LDAP, Kerberos, etc
  - SMB file sharing over IPv6 tunnel interfaces (e.g. ISATAP, 6to4)
  - FTP Server
  - IPHLPAPI IPv6, can't add IPv6 routes via API
  - Many command line tools that show or use explicit IP addresses

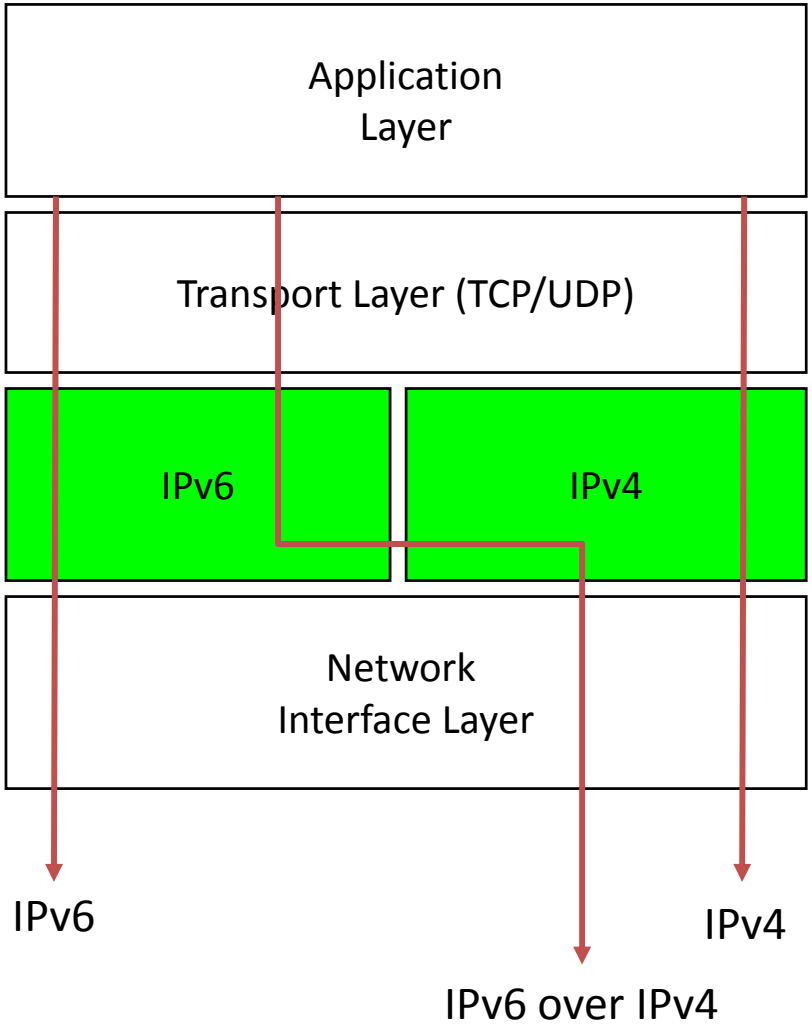
Install IPv6 protocol for Windows Server 2003:

- 1.Log on to the computer with a user account that has privileges to change network configuration.
- 2.Click **Start**, click **Control Panel**, and then double-click **Network Connections**.
- 3.Right-click any local area connection, and then click **Properties**.
- 4.Click **Install**.
- 5.In the Select Network Component Type dialog box, click **Protocol**, and then click **Add**.
- 6.In the Select Network Protocol dialog box, click **Microsoft TCP/IP version 6**, and then click **OK**.
- 7.Click **Close** to save changes to your network connection.

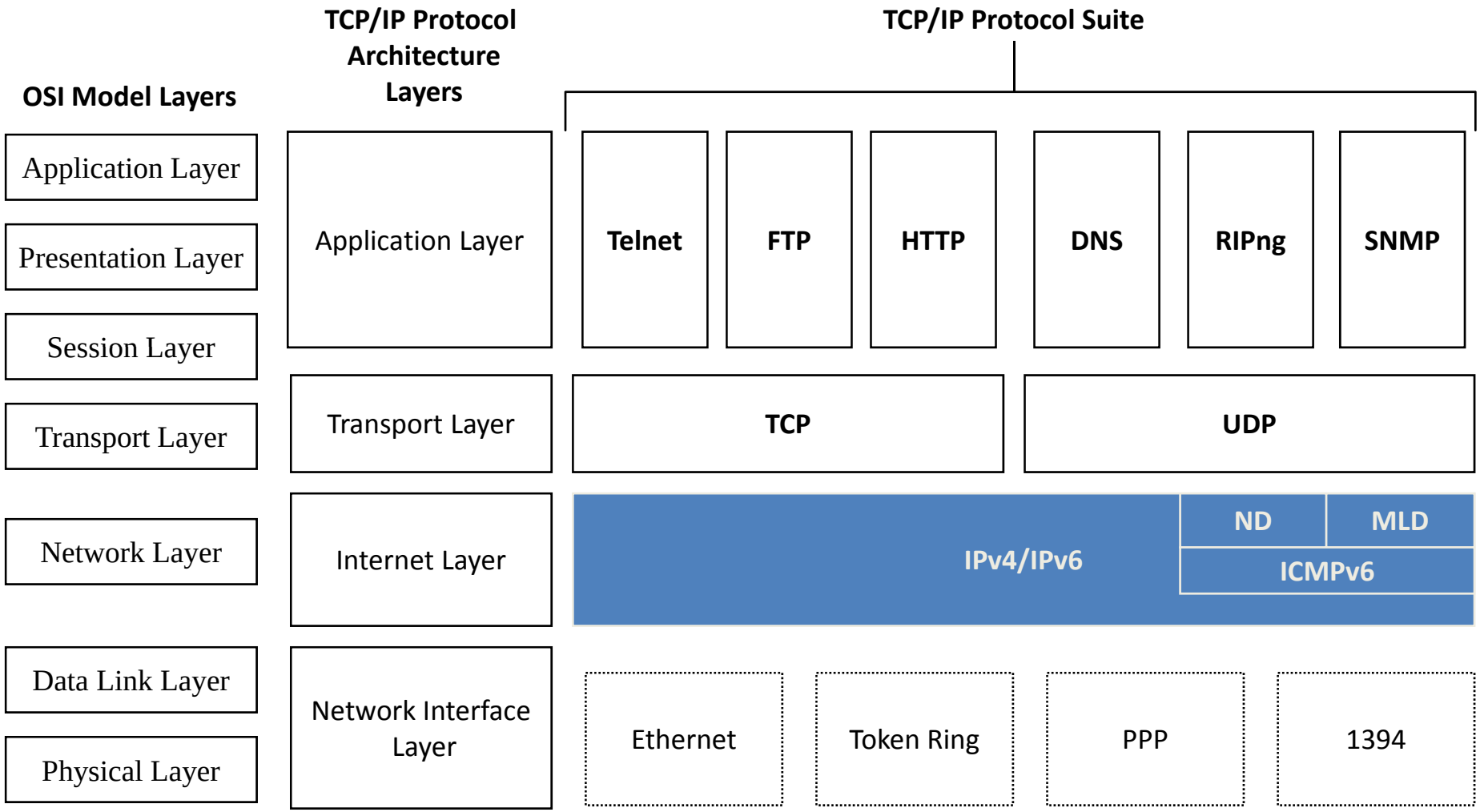
Install IPv6 protocol for Windows XP with SP2:

- 1.Log on to the computer with a user account that has privileges to change network configuration.
- 2.Click **Start**, click **Control Panel**, and then double-click **Network Connections**.
- 3.Right-click any local area connection, and then click **Properties**.
- 4.Click **Install**.
- 5.In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.
- 6.In the **Select Network Protocol** dialog box, click **Microsoft TCP/IP version 6**, and then click **OK**.
- 7.Click **Close** to save changes to your network connection.
- Alternately, from the Windows XP desktop, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**. At the command prompt, type **netsh interface ipv6 install**.

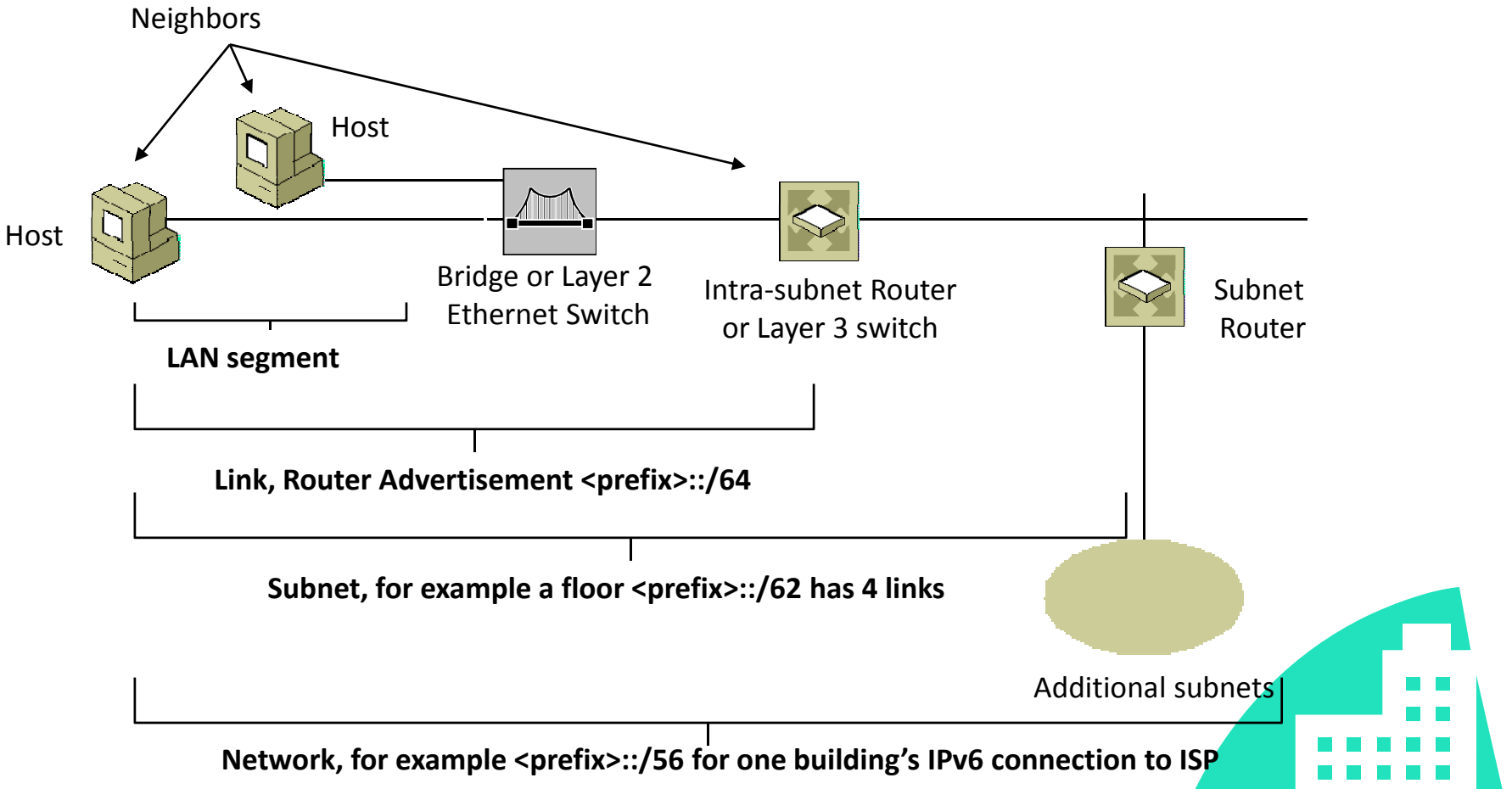
Dual IP Layer Architecture Traffic Types



TCP/IP Protocol Architecture w/IPv6



IPv6 Terminology



LIR/ISP prefix allocation: /48 or /56 for "end-site", "end-user"

Types of IPv6 Addresses

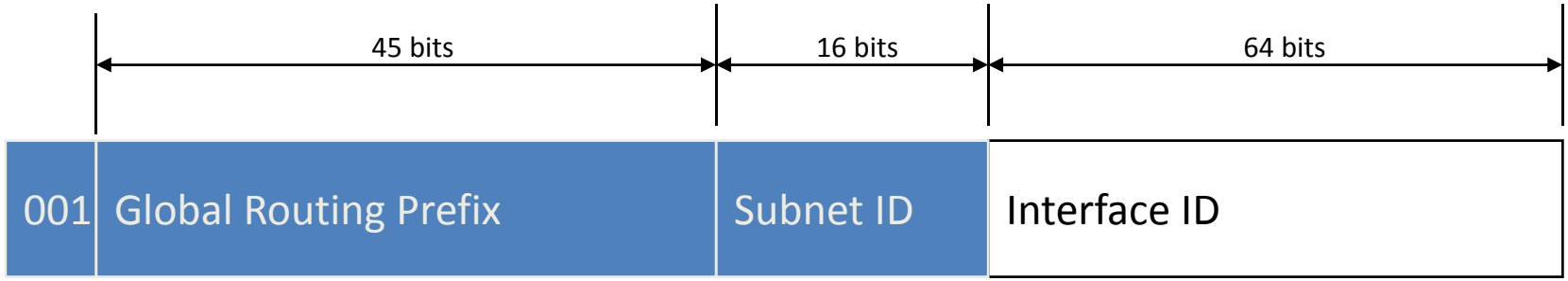
- Unicast
  - Address of a single interface
  - Delivery to single interface
- Multicast
  - Address of a set of interfaces
  - Delivery to all interfaces in the set
- Anycast
  - Address of a set of interfaces
  - Delivery to a single interface in the set
- No more broadcast addresses

Unicast IPv6 Addresses

- Global addresses
- Link-local addresses
- Site-local addresses

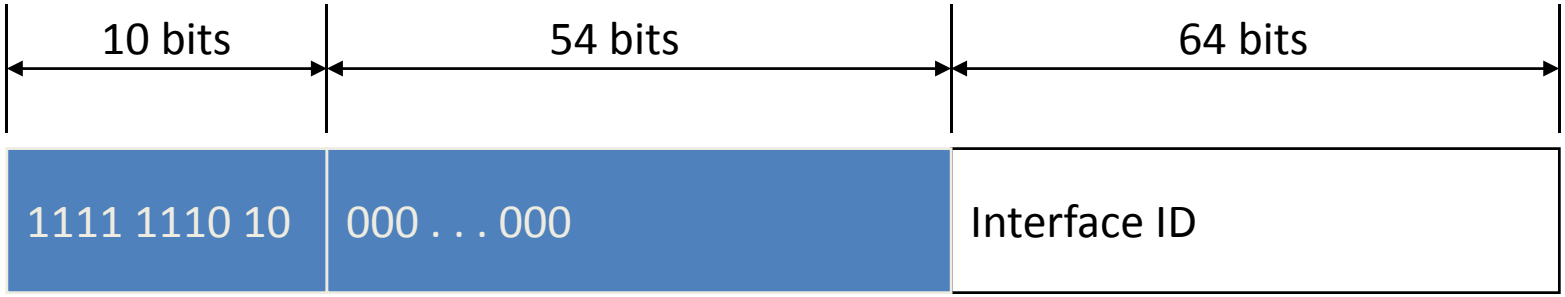
Global Addresses

- Address scope is the entire IPv6 Internet
  - Equivalent to public IPv4 addresses
- Defined in RFC 3587
- Structure
  - Global Routing Prefix
  - Subnet ID
  - Interface ID



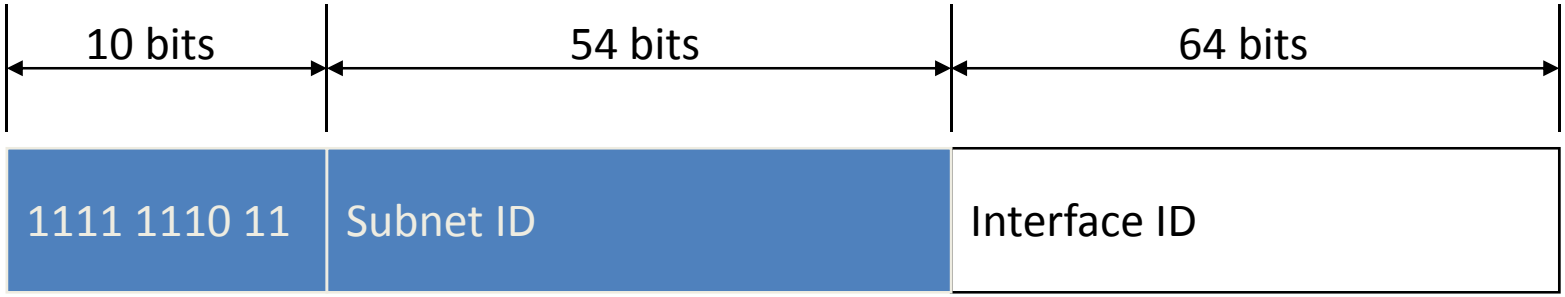
Link-Local Addresses

- Address scope is a single link
  - Equivalent to APIPA IPv4 addresses
- FE80::/64 prefix
- Used for:
  - Single subnet, routerless configurations
  - Neighbor Discovery processes



Site-Local Addresses

- Address scope is a single site
  - Equivalent to private IPv4 addresses
- FEC0::/10 prefix
- Used for intranets that are not connected to the IPv6 Internet
- Recently deprecated but supported for current implementations



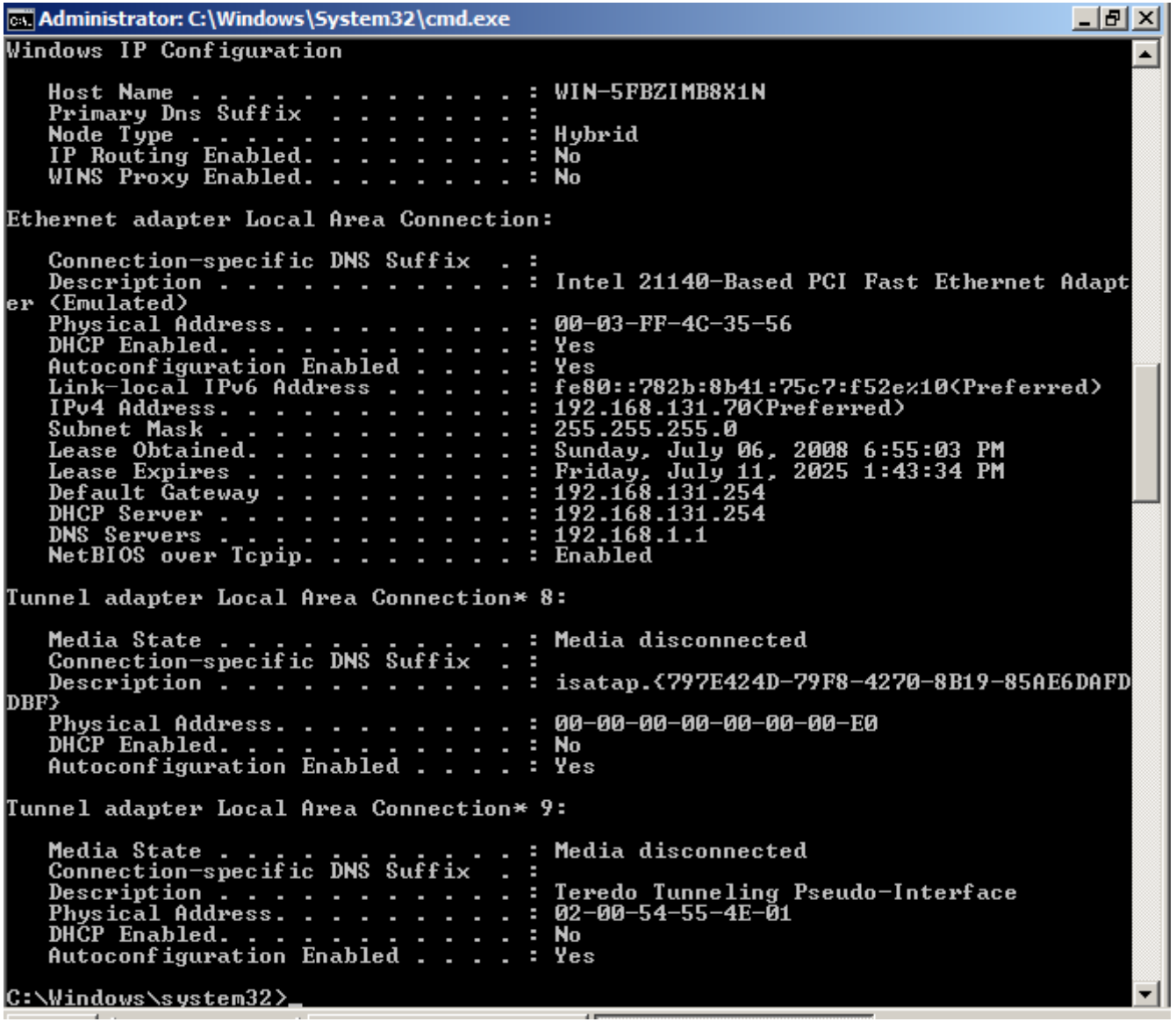
Zone IDs for Link-Local and Site-Local Addresses

- Link-local and site-local addresses are ambiguous
  - Multiple links (common)
  - Multiple sites (uncommon)
- Zone ID is used to identify a specific link or site
  - Link-local address
    - Zone ID is typically set to the interface index of the sending interface
  - Site-local address
    - Zone ID is typically 1 unless multiple sites are used
- Examples:
  - ping fe80::2b0:d0ff:fee9:4143%3
  - tracert fec0::f282:2b0:d0ff:fee9:4143%2

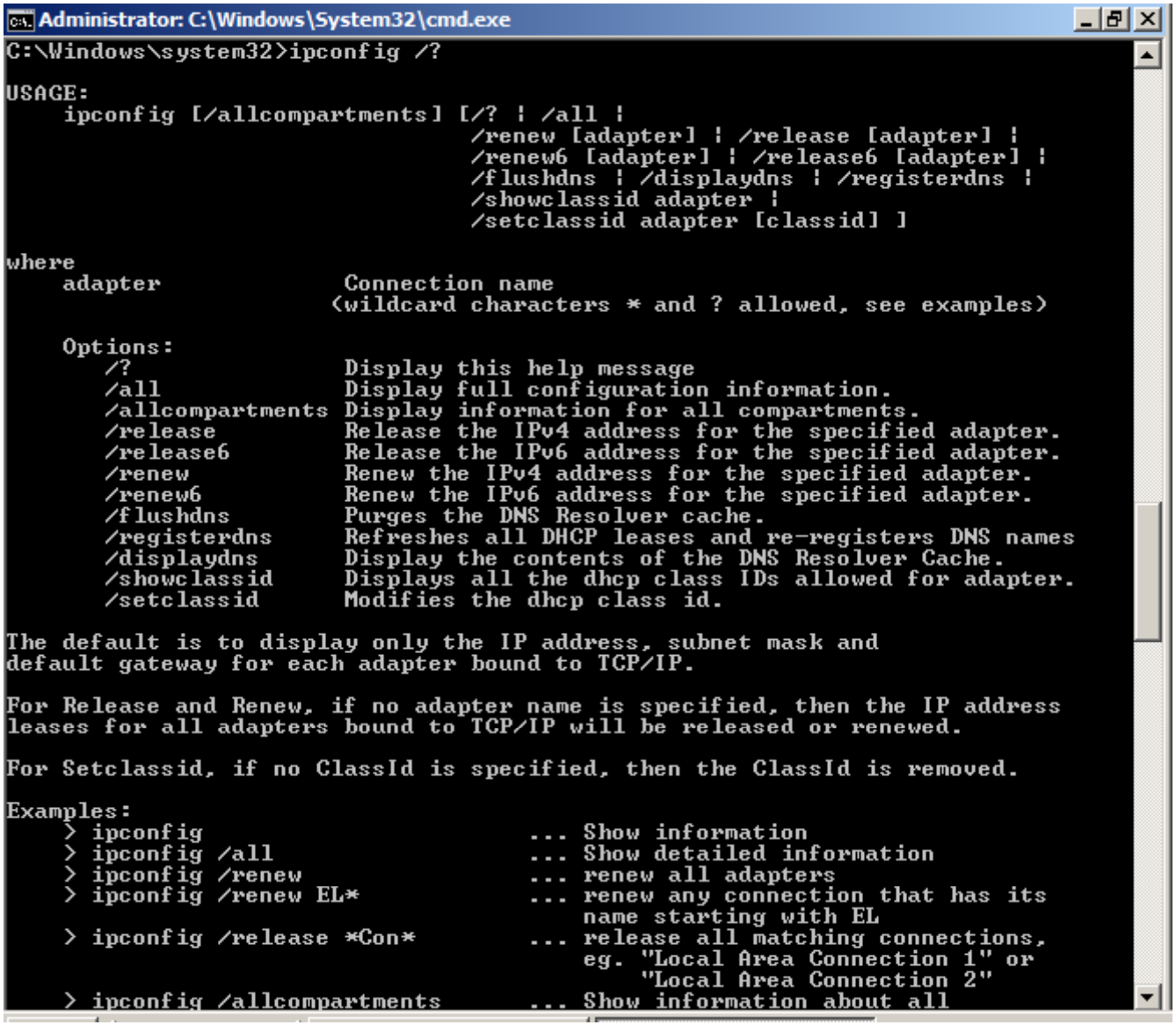
Example of IPv6 addresses

Tunnel adapter 6to4 Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . : redmond.corp.microsoft.com
IP Address. . . . . : 2002:9d3b:9dd5::9d3b:9dd5
Tunnel adapter Automatic Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . : redmond.corp.microsoft.com
IP Address. . . . . : fec0::f70f:0:5efe:157.59.157.213%1
IP Address. . . . . : 3ffe:8311:ffff:f70f:0:5efe:157.59.157.213
IP Address. . . . . : fe80::5efe:157.59.157.213%2
Default Gateway . . . . . : fe80::5efe:157.56.253.8%2

Ipconfig /all



Ipconfig


Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>ipconfig /?
USAGE:
ipconfig [/allcompartments] [/? | /all |
/renew [adapter] | /release [adapter] |
/renew6 [adapter] | /release6 [adapter] |
/flushdns | /displaydns | /registerdns |
/showclassid adapter |
/setclassid adapter [classid]]
where
adapter Connection name
(wildcard characters * and ? allowed, see examples)
Options:
/? Display this help message
/all Display full configuration information.
/allcompartments Display information for all compartments.
/release Release the IPv4 address for the specified adapter.
/release6 Release the IPv6 address for the specified adapter.
/renew Renew the IPv4 address for the specified adapter.
/renew6 Renew the IPv6 address for the specified adapter.
/flushdns Purges the DNS Resolver cache.
/registerdns Refreshes all DHCP leases and re-registers DNS names
/displaydns Display the contents of the DNS Resolver Cache.
/showclassid Displays all the dhcp class IDs allowed for adapter.
/setclassid Modifies the dhcp class id.
The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.
For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.
For Setclassid, if no ClassId is specified, then the ClassId is removed.
Examples:
> ipconfig ... Show information
> ipconfig /all ... Show detailed information
> ipconfig /renew ... renew all adapters
> ipconfig /renew EL* ... renew any connection that has its
name starting with EL
> ipconfig /release *Con* ... release all matching connections,
eg. "Local Area Connection 1" or
"Local Area Connection 2"
> ipconfig /allcompartments ... Show information about all

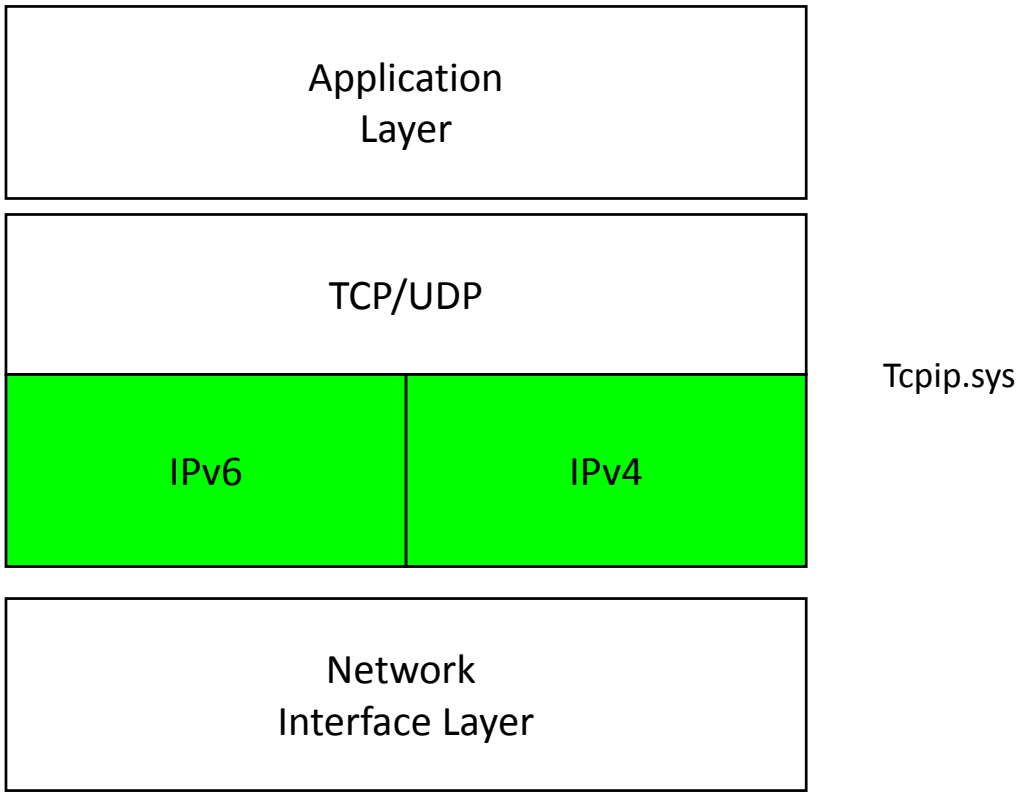
Automatic Tunneling Technologies

- 6to4
  - Allows IPv4/IPv6 hosts to communicate across the IPv4 Internet using public IPv4 addresses
- Teredo (IPv6 NAT Traversal)
  - Allows IPv4/IPv6 hosts to communicate across the IPv4 Internet across NATs
- ISATAP
  - Allows IPv4/IPv6 hosts to communicate across a private IPv4 intranet

Práctico, configuración de:

- 1 – Configurar dirección IP
- 2 – DNS
- 3 – DHCP
- 4 – Internet Information Server
- 5 – Herramientas de diagnóstico

Dual IP Layer Architecture



- Next-Generation TCP/IP stack in Windows Vista/Server “Longhorn”

IPv6 Security Considerations: Transition Technologies (ISATAP)

- ISATAP: Intra-Site Automatic Tunnel Addressing Protocol
  - Easy IPv6 deployment within a site* without upgrading routers
  - Encapsulates IPv6 packets in IPv4 (protocol 41)
- Without explicit ISATAP server deployment
  - Only link local ISATAP addresses configured
  - Reach ability limited to that of only the underlying IPv4 address
  - ISATAP addresses are not registered in DNS
  - Does not trigger AAAA DNS queries
  - ISATAP address derived completely from IPv4 address
    - No more info exposed than already exposed by underlying IPv4 address
- Contained within a site completely by blocking IPv4 protocol 41 at the edge firewall or router

ISATAP can be safely left ON on Windows Vista

IPv6 Security Considerations: Transition Technologies (6to4)

- 6to4
  - Enables two sites and/or hosts connected by global routeable IPv4 Internet to communicate using IPv6
  - Encapsulates IPv6 traffic in protocol 41 IPv4
- Without explicit 6to4 router deployment
  - For hosts without public IPv4 addresses, disabled by default
  - For hosts with public IPv4 addresses, enabled but
    - 6to4 address completely derived from underlying IPv4 address
    - No additional information exposed that is not already exposed by the underlying IPv4 address
- Contained within a site completely by blocking IPv4 protocol 41 at the edge firewall or router

6to4 can be safely left ON on Windows Vista

IPv6 Security Considerations: Transition Technologies (Teredo)

- Teredo
  - Enables two hosts behind NATs to communicate using IPv6
  - Encapsulates IPv6 packets in UDP/IPv4 packets
  - Primarily a consumer technology
- Teredo does not pose security risks for enterprises
  - For domain joined machines, disabled by default
  - For non-domain joined machines, completely blocked by
    - Blocking IPv4 traffic with source or destination UDP port of 3544 at the edge IPv4 firewall or
    - Blocking DNS queries to teredo.ipv6.microsoft.com
  - Not discoverable by DNS, neither causes AAAA queries to be issued