# Chapter 6: Enterprise Internet Connectivity

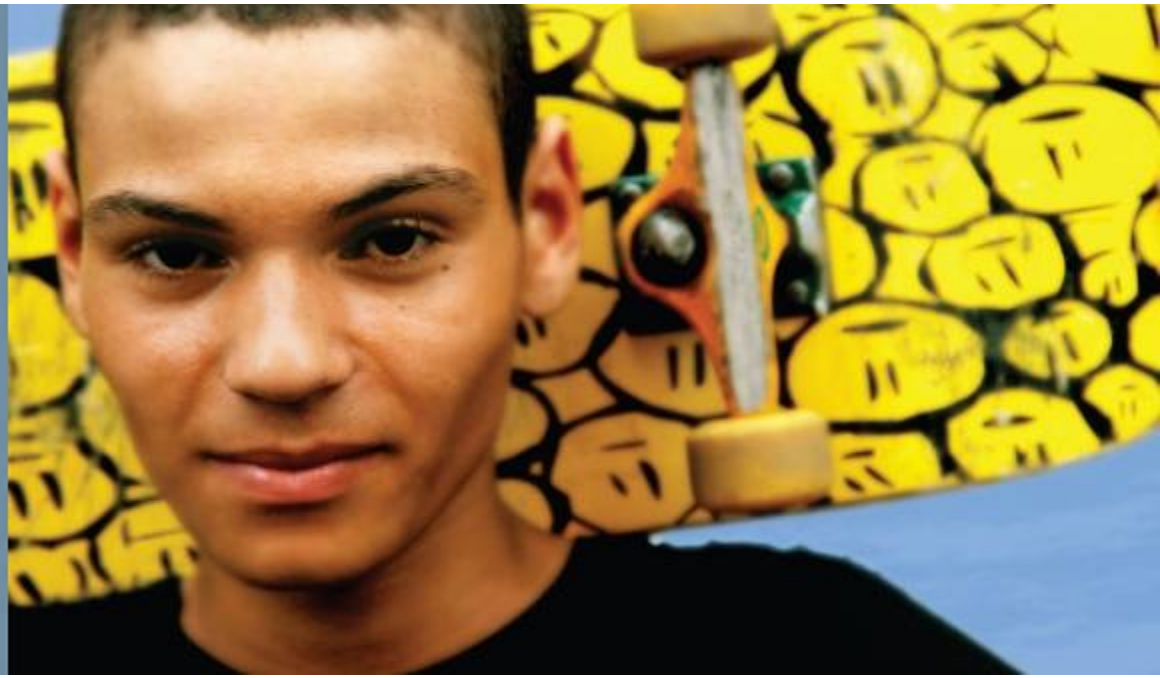
## CCNP ROUTE: Implementing IP Routing

Cisco | Networking Academy®
Mind Wide Open™

# Chapter 6 Objectives

- Planning Enterprise Internet Connectivity
- Establishing Single-Homed IPv4 Internet Connectivity
- Establishing Single-Homed IPv6 Internet Connectivity
- Improving Internet Connectivity Resilience

# Planning Enterprise Internet Connectivity



# Planning Enterprise Internet Connectivity

- Identify the Internet connectivity needs of organizations
- Identify the different types of ISP connectivity
- Describe public IP address assignments and the need for provider-independent IP addressing
- Describe autonomous system numbers

# Connecting Enterprise Networks to an ISP

## Enterprise Connectivity Requirements

- **Outbound**
  - In the rare case that only one-way connectivity outbound from clients to the Internet is required, private IPv4 addresses with Network Address Translation (NAT) are used for IPv4 connections, allowing clients on a private network to communicate with servers on the public Internet.
- **Inbound**
  - Two-way connectivity is needed, so that clients external to the enterprise network can access resources in the enterprise network. In this case, both public and private IPv4 address space is needed, as are routing and security considerations.

# Redundancy for Enterprise Network to ISP connectivity

- **Edge device redundancy**
  - Deploying redundant edge devices, such as routers, protects your network against device failure. If one router fails, Internet connectivity can still be established through the redundant router.
- **Link redundancy**
  - Using redundant links protects your network against link failure between your router and the ISP router.
- **ISP redundancy**
  - If you are hosting important servers in your network or accessing mission-critical servers in the Internet, it is best to have two redundant ISPs. If a failure occurs in one ISP network, traffic can be automatically rerouted through the second ISP.

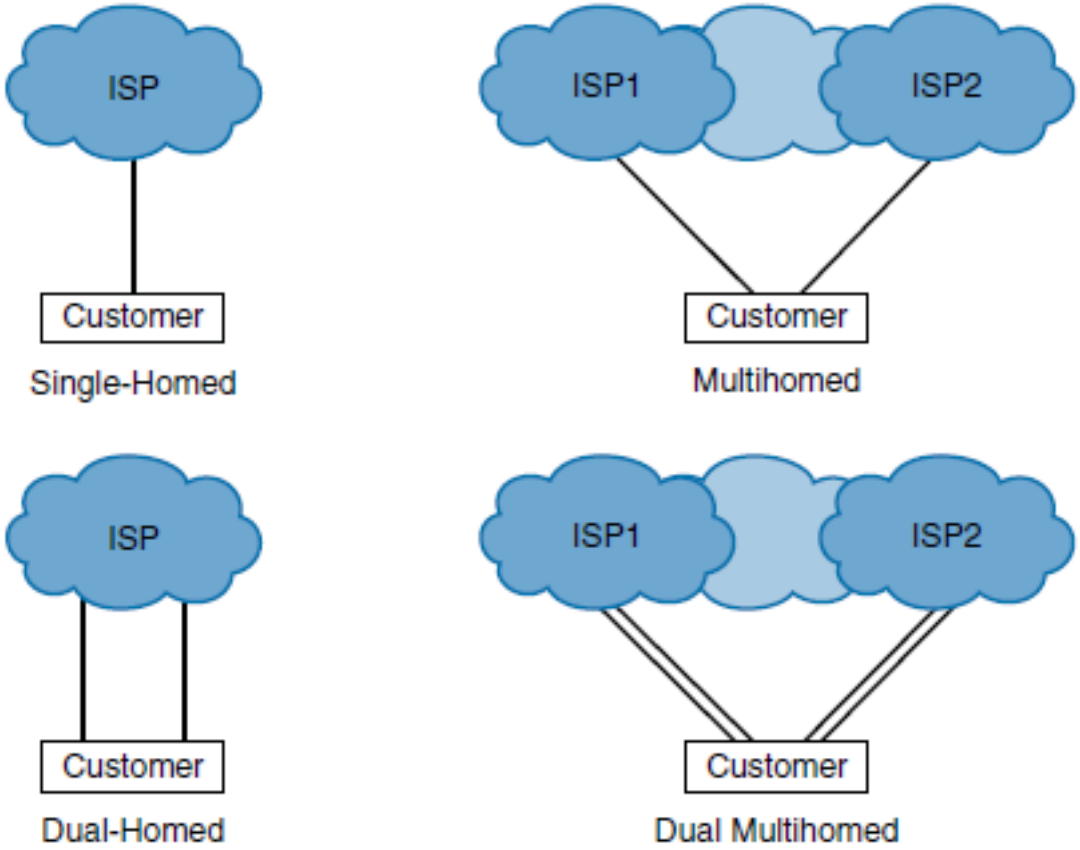
# ISP Redundancy

- **Single-homed**
  - With a connection to a single ISP when no link redundancy is used, the customer is *single-homed.* Single-homed ISP connectivity is used in cases when a loss in Internet connectivity is not problematic to a customer.
- **Dual-homed**
  - With a connection to a single ISP, redundancy can be achieved if two links toward the same ISP are used effectively.
  - There are two options for dual homing: Both links can be connected to one customer router, or to enhance the resiliency further, the two links can terminate at separate routers in the customer's network.
  - In either case, routing must be properly configured to allow both links to be used.

# ISP Redundancy

- **Multihomed**
  - With connections to multiple ISPs, redundancy is built in to the design.
  - Connections from different ISPs can terminate on the same router, or on different routers to further enhance the resiliency.
  - The customer is responsible for announcing its own IP address space to upstream ISPs, but should avoid forwarding any routing information between ISPs (otherwise the customer becomes a transit provider between the two ISPs). The routing used must be capable of reacting to dynamic changes. Multihoming also allows load balancing of traffic between ISPs.
- **Dual multihomed**
  - To enhance the resiliency further with connections to multiple ISPs, a customer can have two links toward each ISP.

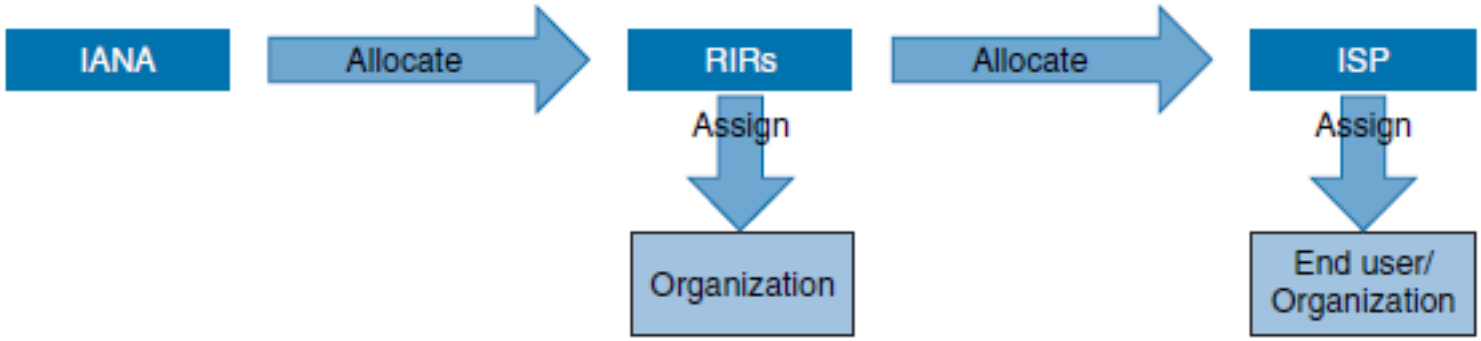
# ISP Redundancy



# Public IP Address Assignment

**The Internet Assigned Numbers Authority (IANA):**

- Coordinate the global pool of IPv4 and IPv6 addresses, and provide them to RIRs (Regional Internet Registries)
- Coordinate the global pool of autonomous system (AS) numbers and provide them to RIRs
- Manage the Domain Name Service (DNS) root zone
- Manage the IP numbering systems (in conjunction with standards bodies)



# Regional Internet Registries (RIRs)

- **African Network Information Centre (AfriNIC)**
  - Responsible for the continent of Africa
- **Asia Pacific Network Information Centre (APNIC)**
  - Administers the numbers for the Asia Pacific region
- **American Registry for Internet Numbers (ARIN)**
  - Has jurisdiction over assigning numbers for Canada, the United States, and several islands in the Caribbean Sea and North Atlantic Ocean
- **Latin American and Caribbean IP Address Regional Registry (LACNIC)**
  - Responsible for allocation in Latin America and portions of the Caribbean
- **Reséaux IP Européens Network Coordination Centre (RIPE NCC)**
  - Administers the numbers for Europe, the Middle East, and Central Asia

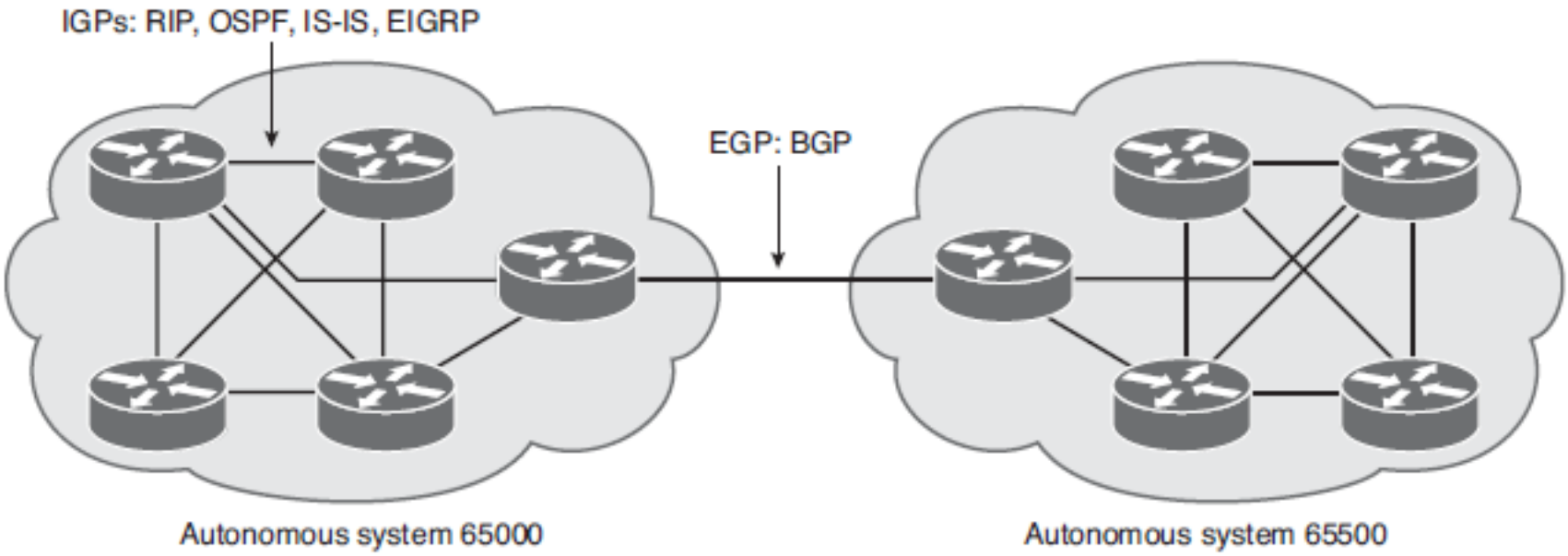
# Public IP Address Space

- **Provider Aggregatable (PA) Address Space**
  - PA address space is a block of IP addresses assigned by a RIR to an ISP which can be aggregated into a single route advertisement for improved Internet routing efficiency.
  - A PA block of IP addresses is used in simple topologies, where no redundancy is needed.
  - PA address space is assigned by the ISP to its customer, from its address space.
  - If the customer changes its ISP, the new ISP will give the customer a new PA address space, and all devices with public IP addresses will have to be renumbered; the old address space cannot be transferred to the new.

# Public IP Address Space

- **Provider-Independent (PI) Address Space**
  - For a multihomed connection, a PI address space is required because the enterprise network needs to be independent of the ISP's address space.
  - The PI address space must be acquired from an RIR; it is assigned directly to an organization by the RIR, and is not related to any ISP.
  - This address space can be routed through other service providers, resulting in more flexibility when planning connections to ISPs and when migrating between service providers.
  - After successfully processing an address space request, the RIR assigns the PI address space and a public autonomous system number (ASN) (described in the next section) that uniquely defines the enterprise's network and its address spaces.
  - This ASN is not related to any ISP.
  - The enterprise then configures their Internet gateway routers to advertise the newly assigned IP address space to neighboring ISPs; the Border Gateway Protocol (BGP) is typically used for this task.

# Autonomous System Numbers




- The ASN is a very important parameter required when configuring BGP.

# A complete table of 16-bits and 32-bits ASN available

| Number | Bits | Description | Reference |
|---|---|---|---|
| 0 | 16 | Reserved for RPKI unallocated space invalidation[19] | RFC 6483, RFC 7607 |
| 1 - 23455 | 16 | Public ASNs | |
| 23456 | 16 | Reserved for AS Pool Transition | RFC 6793 |
| 23457 - 64495 | 16 | Public ASNs | |
| 64496 - 64511 | 16 | Reserved for use in documentation and sample code | RFC 5398 |
| 64512 - 65534 | 16 | Reserved for private use | RFC 1930, RFC 6996 |
| 65535 | 16 | Reserved | RFC 7300 |
| 65536 - 65551 | 32 | Reserved for use in documentation and sample code | RFC 5398, RFC 6793 |
| 65552 - 131071 | 32 | Reserved | |
| 131072 - 4199999999 | 32 | Public 32-bit ASNs | |
| 4200000000 - 4294967294 | 32 | Reserved for private use | RFC 6996 |
| 4294967295 | 32 | Reserved | RFC 7300 |

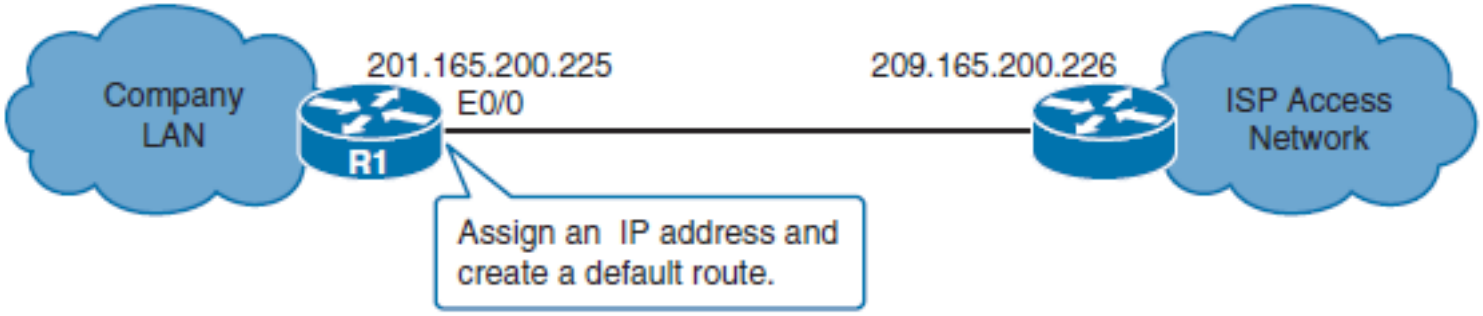
# Establishing Single-Homed IPv4 Internet Connectivity

# Establishing Single-Homed IPv4 Internet Connectivity

- Describe how to configure your router with both a provider-assigned static IPv4 address and a provider-assigned DHCP address
- Understand DHCP operation and describe how to use a router as a DHCP server and relay agent
- Identify the various types of NAT
- Describe the NAT virtual interface (NVI) feature, configuration, and verification

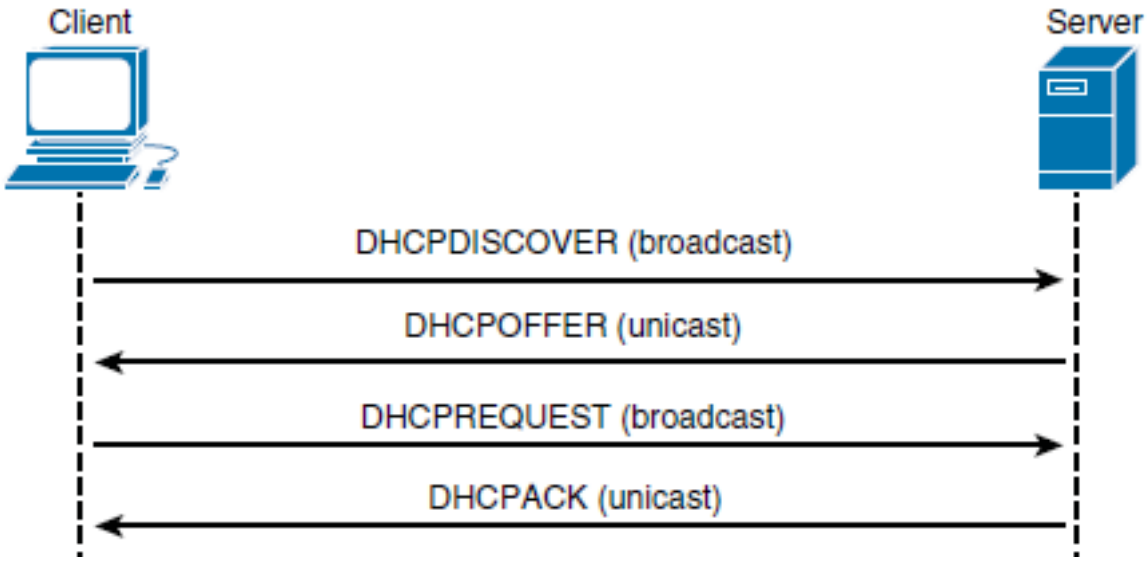
# Configuring a Provider-Assigned IPv4 Address

- **Step 1.** Assign the static IPv4 address on the router's Internet-facing interface.
- **Step 2.** Configure a default route that will forward all traffic intended for the Internet to the ISP.




```
R1(config)# interface Ethernet 0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

# DHCP Operation

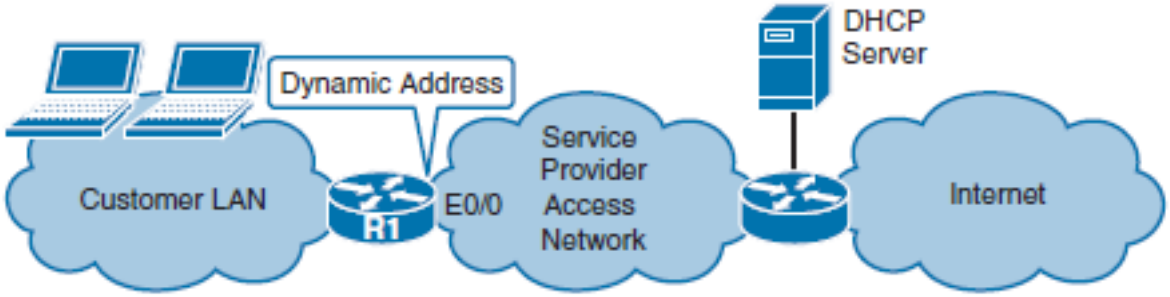



Four other DHCP messages are possible:

- **DHCPDECLINE:** A message sent from a client to a server indicating that the address is already in use
- **DHCPNAK:** A message sent from a server indicating that it is refusing a client's request for configuration
- **DHCPRELEASE:** A message sent from a client indicating to a server that it is giving up a lease
- **DHCPINFORM:** A message sent from a client indicating that it already has an IPv4 address, but is requesting other configuration parameters from the DHCP server, such as a DNS address

# Obtaining a Provider-Assigned IPv4 Address with DHCP

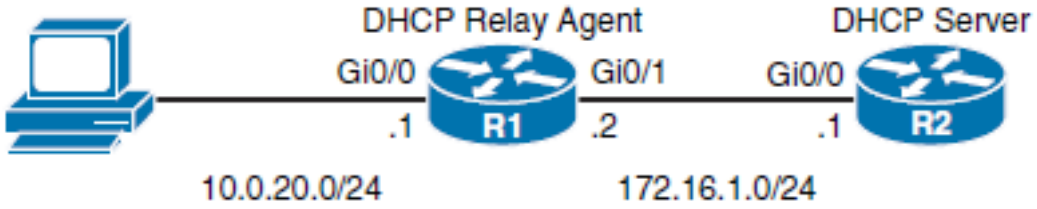
- When dynamic assignment is used by the ISP, no manual address assignment is needed; instead, DHCP client functionality needs to be enabled on the router interface. Other configuration information can also be obtained through DHCP, such as the default gateway address.




```
R1(config)# interface Ethernet 0/0
R1(config-if)# ip address dhcp
R1(config-if)# end

R1# show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "static", distance 254, metric 0, candidate default path
  Routing Descriptor Blocks:
  * 209.165.200.226
      Route metric is 0. traffic share count is 1
```

# Configuring a Router as a DHCP Server and DHCP Relay Agent




```
R2(config)# ip dhcp pool MYLAN
R2(dhcp-config)# network 10.0.20.0 255.255.255.0
R2(dhcp-config)# default-router 10.0.20.1
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp excluded-address 10.0.20.1 10.0.20.49
```

```
R1(config)# interface gi0/0
R1(config-if)# ip helper-address 172.16.1.1
```

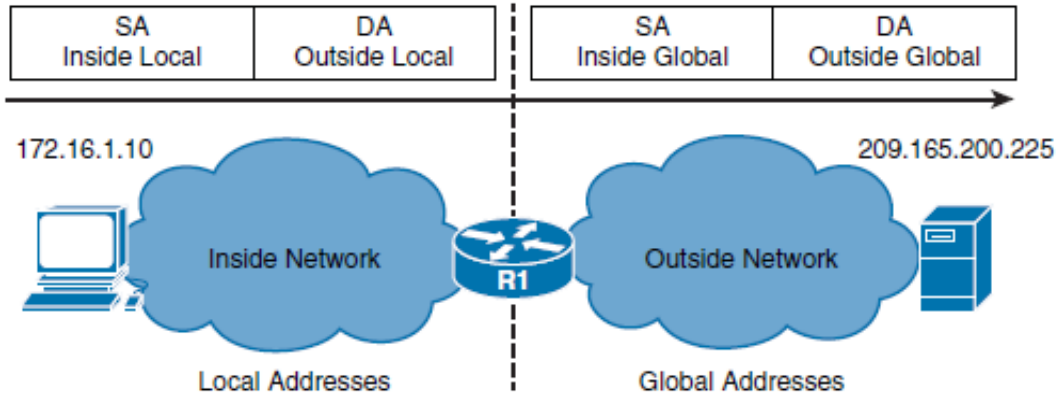
# NAT

- NAT is usually implemented on border devices such as firewalls or routers, which allows devices within an organization to have private addresses.
- NAT translates private addresses to public addresses and vice versa, keeping a mapping between the two for return traffic.
- NAT can be configured to translate all private addresses to only one public address (PAT) or to pick from a pool of public addresses.
- RFC 1918, *Address Allocation for Private Internets* , has set aside the following IPv4 address space for private use:
  - **Class A network:** 10.0.0.0 to 10.255.255.255
  - **Class B network:** 172.16.0.0 to 172.31.255.255
  - **Class C network:** 192.168.0.0 to 192.168.255.255

# NAT

NAT uses the terms *inside* and *outside*. Inside means internal to your network, and outside means external to your network. NAT includes the following four types of addresses:

- **Inside local address**
  - The IPv4 address assigned to a device on the internal network.
- **Inside global address**
  - The IPv4 address of an internal device as it appears to the external network. This is the address to which the inside local address is translated.
- **Outside local address**
  - The IPv4 address of an external device as it appears to the internal network. If outside addresses are being translated, this is the address to which the outside global address is translated.
- **Outside global address**
  - The IPv4 address assigned to a device on the external network.



# Types of NAT

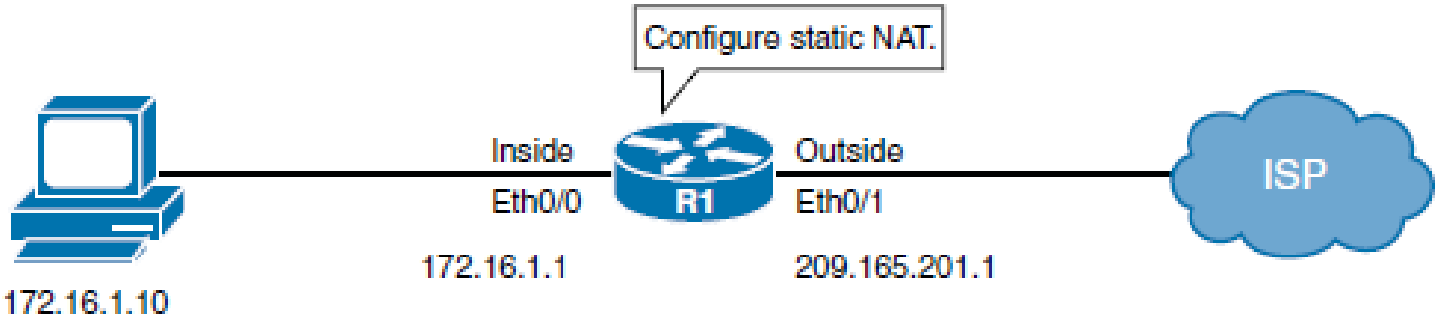
- **Static NAT**
  - Static NAT is one-to-one translation. Static NAT is particularly useful when a device must be accessible from outside the network
- **Dynamic NAT**
  - Dynamic NAT is many-to-many translation, using a pool of addresses. When an inside device accesses an outside network, it is assigned an available IPv4 address from the pool on a first-come, first-serve basis. When using dynamic NAT, you need to ensure that there are enough addresses available in the pool to satisfy the total number of user sessions.
- **Port Address Translation (PAT)**
  - PAT is many-to-one translation; for example, it maps multiple inside local IPv4 addresses to a single inside global IPv4 address by tracking port numbers. PAT is also known as *NAT overloading* .

# Configuring Static NAT

- Using the **`ip nat inside source static`** *`local-ip global-ip`* global configuration command.

| Parameter | Description |
|---|---|
| *local-ip* | The inside local IPv4 address assigned to a host on the inside network. |
| *global-ip* | The inside global IPv4 address of an inside host as it appears to the outside world |

# Configuring Static NAT - Example




```
Router(config)# interface Ethernet 0/1
Router(config-if)# ip address 209.165.201.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source static 172.16.1.10 209.165.201.5
```

# Configuring Dynamic NAT

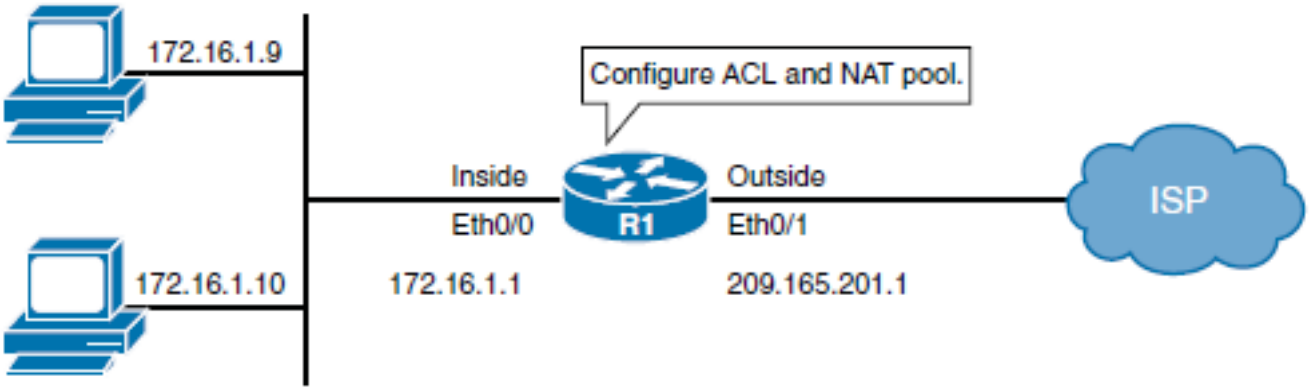
- **ip nat pool** *{name}* **start-ip** *ip* **end-ip** *ip* **{netmask | prefix}**

| Parameter | Description |
|---|---|
| *name* | Name of the pool |
| *start-ip* | Starting IPv4 address that defines the range of addresses in the address pool |
| *end-ip* | Ending IPv4 address that defines the range of addresses in the address pool |
| *netmask* | Specifies the subnet mask of the network to which the pool addresses belong |
| *prefix-length* | Alternative way of specifying the subnet mask of the network to which the pool addresses belong |

- **ip nat inside source list** { *access-list-number* | *access-list-name* } **pool** *name*

| Parameter | Description |
|---|---|
| *access-list-number* | Identifies a standard IPv4 access list. The source address of packets that are permitted by the access list is dynamically translated to an inside global addresses from the named pool. |
| *access-list-name* | Identifies a standard IPv4 access list. The source address of packets that are permitted by the access list is dynamically translated to an inside global addresses from the named pool. |
| *name* | Name of the pool from which the inside global IPv4 addresses are dynamically allocated. |

# Configuring Dynamic NAT - Example



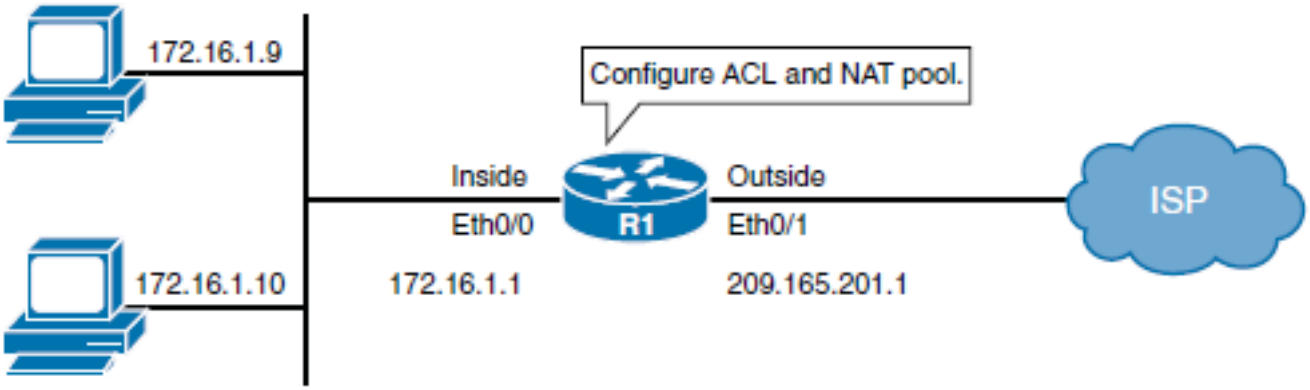

```
Router(config)# access-list 1 permit 172.16.1.0 0.0.0.255
Router(config)# ip nat pool NAT-POOL 209.165.201.5 209.165.201.10
  netmask 255.255.255.240
Router(config)# interface Ethernet 0/1
Router(config-if)# ip address 209.165.201.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)#exit
Router(config)# ip nat inside source list 1 pool NAT-POOL
```

# Configuring PAT

- **ip nat inside source list** { *access-list-number* | *access-list-name* } { **interface** *type number* } [ **overload** ]

| Parameter | Description |
|---|---|
| *access-list-number* | Identifies a standard IP access list. The source address of packets that are permitted by the access list is translated to the address of the specified interface. |
| *access-list-name* | Identifies a standard IP access list. The source address of packets that are permitted by the access list is translated to the address of the specified interface. |
| *type number* | Specifies the interface type and number from which the inside global address will be taken. |
| overload | (Optional) Enables the router to use one inside global address for many inside local addresses. When overloading is configured, the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address. |

# Configuring PAT - Example



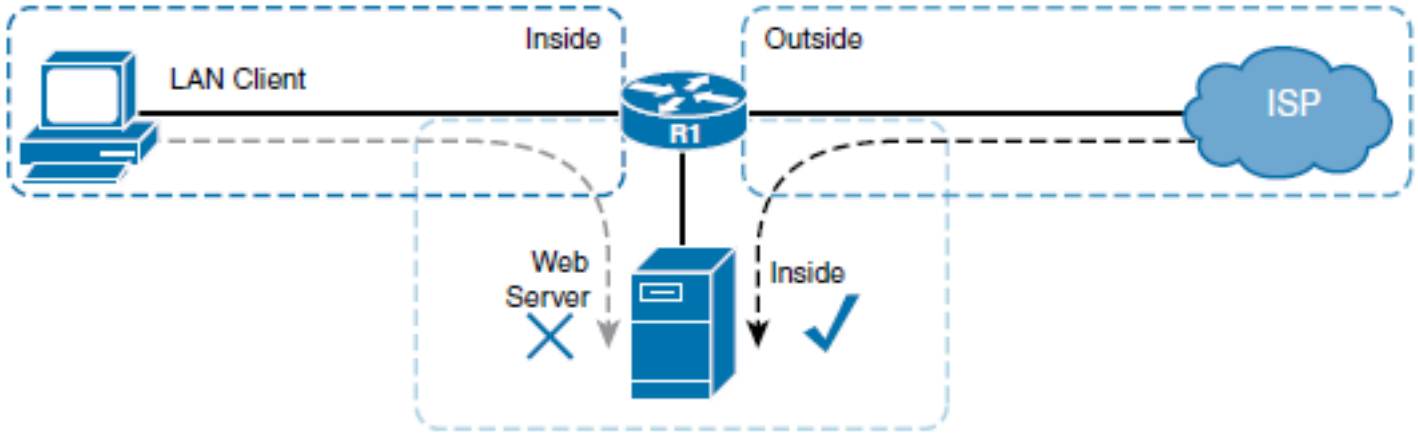

```
Router(config)# access-list 1 permit 172.16.1.0 0.0.0.255
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# interface Ethernet 0/1
Router(config-if)# ip address 209.165.201.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# ip nat inside source list 1 interface Ethernet 0/1 overload
```

# Limitations of NAT

- **End-to-end visibility issues:** Many applications depend on end-to-end functionality, with unmodified packets being forwarded from source to destination. By changing end-to-end addresses, NAT effectively blocks such applications.
- **Tunneling becomes more complex:** Using NAT can complicate tunneling protocols, such as IPsec, because NAT modifies the values in the headers and thus interferes with the integrity checks done by IPsec and other tunneling protocols.

# Limitations of NAT

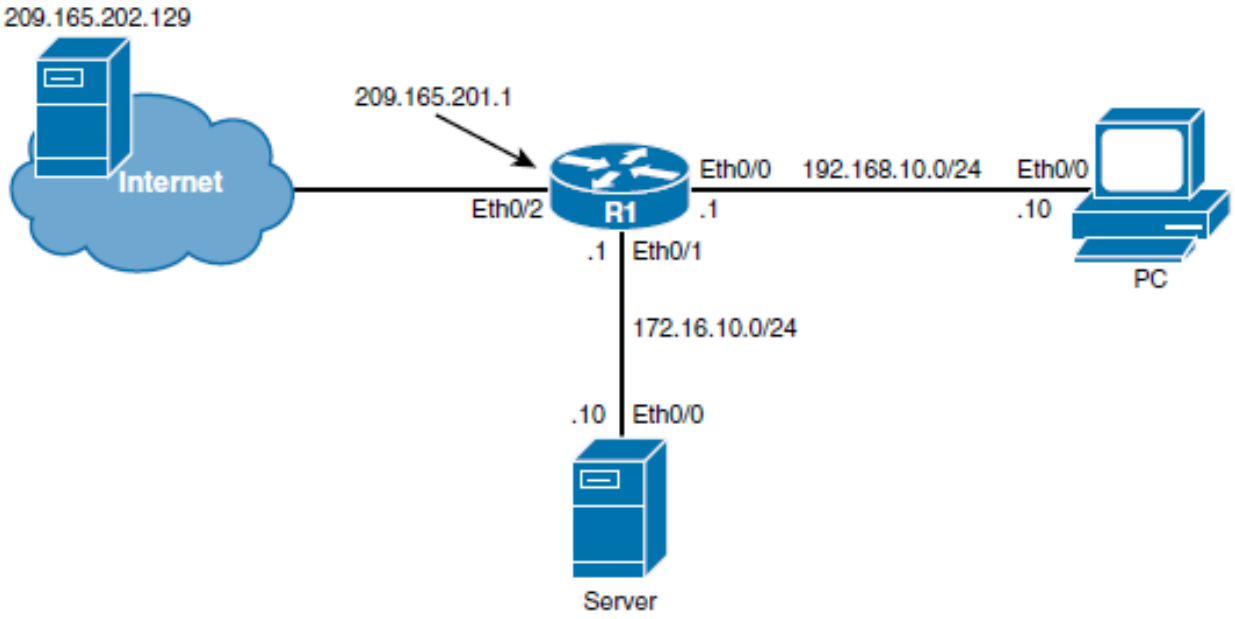
- **In certain topologies, standard NAT may not work correctly**
  - R1 router is configured to perform PAT for the LAN clients and static NAT for the web server.
  - When a client on the Internet wants to access the web server, it gets the server's public IP address from the DNS. The router statically translates the server's public IP address to its inside local address, and forwards packets to the server.
  - When a client on the LAN tries to access the server, it similarly gets the same public IP address for the server from DNS, and tries to access the server. However, attempts to connect to the server will fail because of how NAT operates.
  - When packets go from inside to outside, they are first routed and then translated; the packets from the LAN client are routed to the outside interface and the LAN client's address is translated by PAT. When packets travel from outside to inside, they are translated and routed. In this case however, the packets from the LAN client do not come into the router's outside interface; therefore, they are never translated so they are never routed back to the interface where the server is located.
  - The result is that the LAN client cannot connect to the web server.



# NAT Virtual Interface

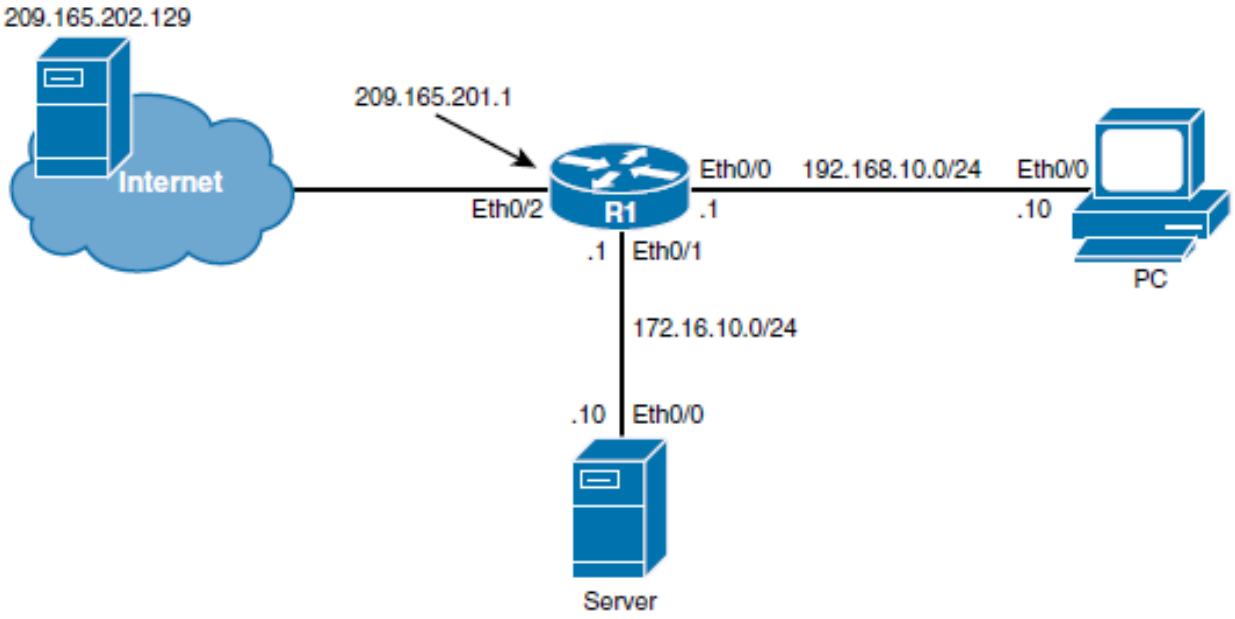
- As of Cisco IOS Software Release 12.3(14)T Cisco introduced a new feature, NAT virtual interface (NVI), which removes the requirement to configure an interface as inside or outside.
- The NVI order of operations is also slightly different than NAT.
- Recall that classic NAT first performs routing and then translation when going from an inside interface to an outside interface, and vice versa when the traffic flow is reversed.
- NVI, however, performs routing, translation, and routing again; NVI performs the routing operation twice, before and after translation, before forwarding the packet to an exit interface.
- The whole process is symmetrical, no matter which way the traffic is flowing.
- Because of the added routing step, packets can flow, in classic NAT terms, from an inside to an inside interface; as described in the previous section, this scenario fails if classic NAT is used.

# Configuring NAT Virtual Interface




```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# ip nat pool TEST1 209.165.201.5 209.165.201.10 prefix-length 27
R1(config)# ip nat source list 10 pool TEST1
R1(config)# ip nat source static 172.16.10.10 209.165.201.2
```

# Configuring NAT Virtual Interface




```
R1(config)# interface ethernet 0/0
R1(config-if)# ip nat enable
R1(config-if)# interface ethernet 0/1
R1(config-if)# ip nat enable
R1(config-if)# interface ethernet 0/2
R1(config-if)# ip nat enable
```

# NVI Interface

```
R1# show ip interface brief
Interface        IP-Address      OK?  Method  Status                  Protocol
Ethernet0/0      192.168.10.1    YES  manual  up                      up
Ethernet0/1      172.16.10.1     YES  manual  up                      up
Ethernet0/2      209.165.201.1   YES  manual  up                      up
Ethernet0/3      unassigned      YES  NVRAM   administratively down  down
NVI0             192.168.10.1    YES  unset   up                      up
```

- When a packet enters the NAT router on any NAT-enabled interface, it is matched against the NAT translation table.
- If there is a match, the packet is routed to the NVI0 interface, where translation takes place. After the translation process, the packet is routed again and forwarded to the appropriate interface.
- The NVI0 interface is assigned an IPv4 address, which is needed for Cisco IOS internal operation. The assigned IPv4 address has no influence on NAT behavior; it is copied from the first physical interface or from the first interface on which NAT is enabled.

# show ip nat nvi translations

```
R1# show ip nat nvi translations
Pro Source global       Source local        Destin  local        Destin  global
icmp 209.165.201.2:0    172.16.10.10:0      209.165.202.129:0    209.165.202.129:0
--- 209.165.201.2       172.16.10.10        ---                  ---
icmp 209.165.201.5:0    192.168.10.10:0     209.165.202.129:0    209.165.202.129:0
icmp 209.165.201.5:1    192.168.10.10:1     172.16.10.10:1       172.16.10.10:1
icmp 209.165.201.5:2    192.168.10.10:2     209.165.201.2:2      172.16.10.10:2
--- 209.165.201.5       192.168.10.10       ---                  ---
```

```
R1# show ip nat translations
Pro Inside global   Inside local    Outside local   Outside global
```

# show ip nat nvi statistics

```
R1# show ip nat nvi statistics
Total active translations: 4 (1 static, 3 dynamic; 2 extended)
NAT Enabled interfaces:
  Ethernet0/0, Ethernet0/1, Ethernet0/2
Hits: 34  Misses: 4
CEF Translated packets: 10, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Source [Id: 3] access-list 10 pool TEST1 refcount 2
 pool TEST1: netmask 255.255.255.224
        start 209.165.201.5 end 209.165.201.10
        type generic, total addresses 6, allocated 1 (16%), misses 0
```

# Establishing Single-Homed IPv6 Internet Connectivity

# Establishing Single-Homed IPv6 Internet Connectivity

- Describe the various ways that your router can obtain an IPv6 address
- Understand DHCP for IPv6 (DHCPv6) operation and describe the use of a router as a DHCPv6 server and relay agent
- Describe the use of NAT for IPv6
- Identify how to configure IPv6 ACLs
- Describe the need to secure IPv6 Internet connectivity

# Obtaining a Provider-Assigned IPv6 Address

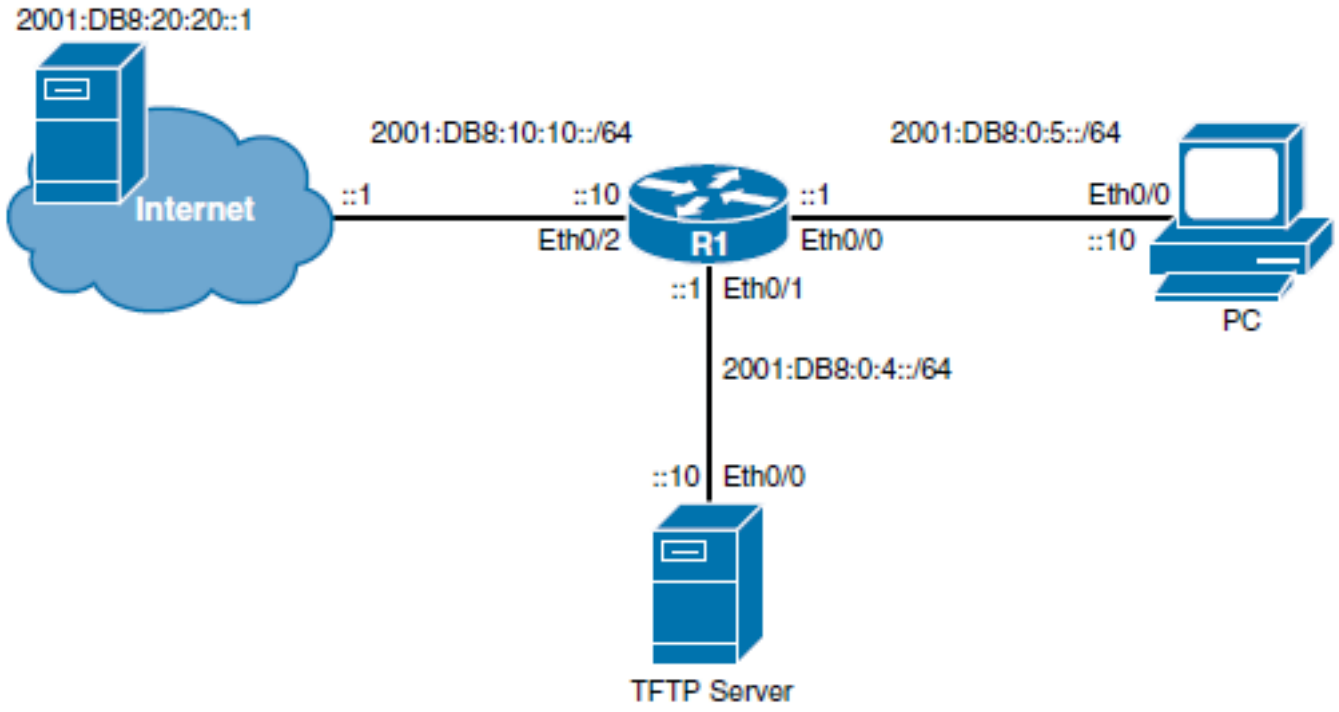
The IPv6 address assignment methods are as follows:

- Manual assignment
- Stateless address autoconfiguration (SLAAC)
- Stateless DHCPv6
- Stateful DHCPv6
- DHCPv6 prefix delegation (DHCPv6-PD)

# Manual Assignment

- As with IPv4, an IPv6 address can be statically assigned by a network administrator.
- This assignment method can be error-prone and introduces significant administrative overhead, especially because of the 128-bit length of IPv6 addresses.

# Configuring Basic IPv6 Internet Connectivity



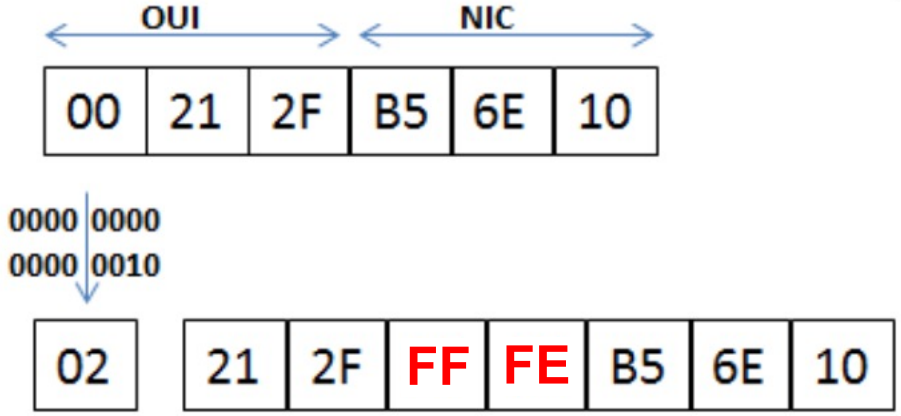

```
R1(config)# ipv6 unicast-routing
R1(config)# interface Ethernet 0/2
R1(config-if)# ipv6 address 2001:DB8:10:10::10/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 route ::/0 2001:DB8:10:10::1
```

# Stateless Address Autoconfiguration

- SLAAC provides the capability for a device to obtain IPv6 addressing information without any intervention from the network administrator.
- This is achieved with the help of RAs (Router Advertisements), which are sent by routers on the local link (by default and periodically).
- RA messages include one or more prefixes, prefix lifetime information, flag information, and default router lifetime information.
- The source IPv6 link-local address of the RA message is used by the host as its IPv6 default router address.
- IPv6 hosts listen for these RAs and use the advertised prefix, which must be 64 bits long.
- The host generates the remaining 64 host bits either by using the IEEE EUI-64 format or by creating a random sequence of bits.
- If the generated IPv6 address is unique, it can be applied to the interface.
- This process introduces plug-and-play functionality to the network, which significantly reduces administrative overhead; however, it provides no way of tracking address assignment.

# IEEE EUI-64

1. The MAC address is split into two 24-bit parts.
2. 0x**FFFE** is inserted between the two parts, resulting in a 64-bit value.
3. The seventh bit of the first octet is inverted. (In a MAC address, this bit indicates the scope and has a value of 0 for global scope and 1 for local scope; it will be 0 for globally unique MAC addresses. In the EUI-64 format used for IPv6 interface IDs, the meaning of this bit is opposite, so the bit is inverted.)



# Enabling SLAAC

- Use the **ipv6 address autoconfig** [ **default** ] interface configuration command to enable automatic configuration of IPv6 addresses using SLAAC.
- The optional **default** keyword causes a default route to be installed using that default router.
- You can specify the **default** keyword on only one interface.
- Note that the commands configured on a router determine when it generates router solicitation (RS) and RA messages:
  - Routers configured with the **ipv6 unicast-routing** command generate RA messages. They do not generate RS messages.
  - Routers configured with the **ipv6 address autoconfig** command, and not configured with the **ipv6 unicast-routing** command, generate RS messages only. They do not generate RA messages.

# DHCPv6 Operation

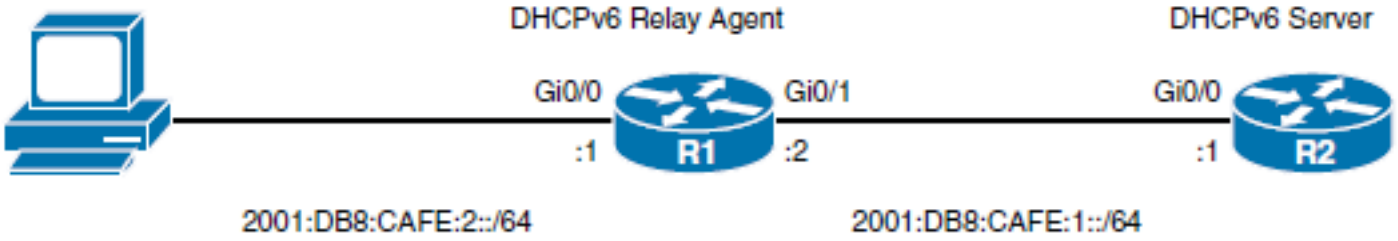
In the IPv6 world, there are two types of DHCPv6:

- **Stateless:** Used to supply additional parameters to clients that already have an IPv6 address
- **Stateful:** Similar to DHCP for IPv4 (DHCPv4)

# Stateless DCHPv6

- Stateless DHCPv6 works in combination with SLAAC.
- An IPv6 host gets its addressing and default router information using SLAAC, from information contained within an RA.
- However, the IPv6 host also queries a DHCPv6 server for other information it needs, such as the DNS or NTP server addresses.
- The query for other configurations is triggered by the *other configuration* flag bit set in the RA.
- In this case, the DHCPv6 server does not assign IPv6 addresses, and therefore does not need to maintain any dynamic state information for the clients; therefore, it is called ***stateless***.

# Configuring Stateless DCHPv6



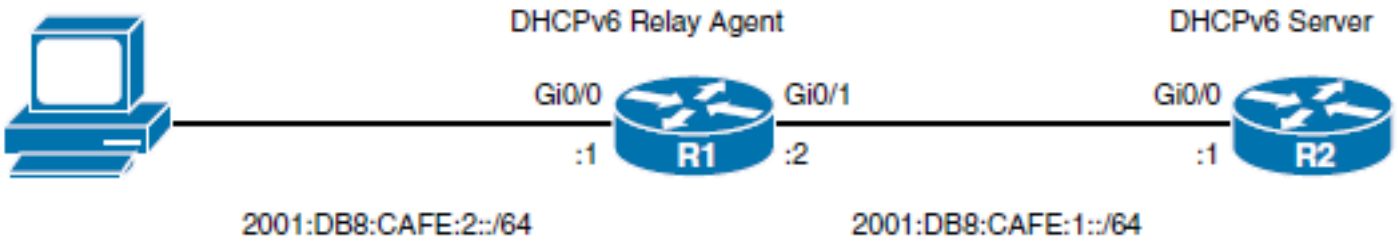

```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 dhcp relay destination 2001:DB8:CAFE:1::1

R2(config)# ipv6 dhcp pool IPV6-STATELESS
R2(config-dhcpv6)# dns-server 2001:DB8:CAFE:1::99
R2(config-dhcpv6)# domain-name www.example.com
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 dhcp server IPV6-STATELESS
```

# Stateful DHCPv6

- When stateful DHCPv6 is implemented, RAs use the *managed address configuration* flag bit to tell IPv6 hosts to get their addressing and additional information only from the DHCPv6 server.
- This flag tells the hosts to disregard the prefixes in the RA and instead query the DHCPv6 server for addressing and other information.
- The DHCPv6 server then allocates addresses to the host and tracks the allocated address.
- Note that the default router address is still received from the RA link-local address.

# Configuring Stateful DHCPv6




```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# ipv6 dhcp relay destination 2001:DB8:CAFE:1::1

R2(config)# ipv6 dhcp pool IPV6-STATEFUL
R2(config-dhcpv6)# address prefix 2001:DB8:CAFE:2::/64
R2(config-dhcpv6)# dns-server 2001:DB8:CAFE:1::99
R2(config-dhcpv6)# domain-name www.example.com
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 dhcp server IPV6-STATEFUL
```

# DHCPv6 Operation

- The client sends a **SOLICIT** message to find a DHCPv6 server and request assignment of addresses and other configuration information.
- This message is sent to the *all-DHCP-agents* multicast address (FF02::1:2) with link-local scope
- Any DHCPv6 servers that can meet the client's requirement respond to the client with an **ADVERTISE** message.
- The client chooses one of the servers and sends a **REQUEST** message to it, asking it to confirm the addresses and other information that were advertised.
- The server responds with a **REPLY** message that contains the confirmed addresses and configuration information.
- Like with DHCPv4, a DHCPv6 client renews its lease after a period of time by sending a RENEW message.
- By default, the four-message exchange is used; when the **rapid-commit** option is enabled by both the client and server, the two-message exchange is used (SOLICIT-REPLY).

# NAT for IPv6

- In IPv4, NAT is typically used to translate private addresses to public addresses when communicating on the Internet. In IPv6, we do not have to worry about private-to-public address translation, but some forms of NAT are still used.

NAT64

- NAT64 performs both address and IP header translation. An example use of NAT64 is to provide IPv4 Internet connectivity to IPv6 devices, during the transition to a full IPv6 Internet.

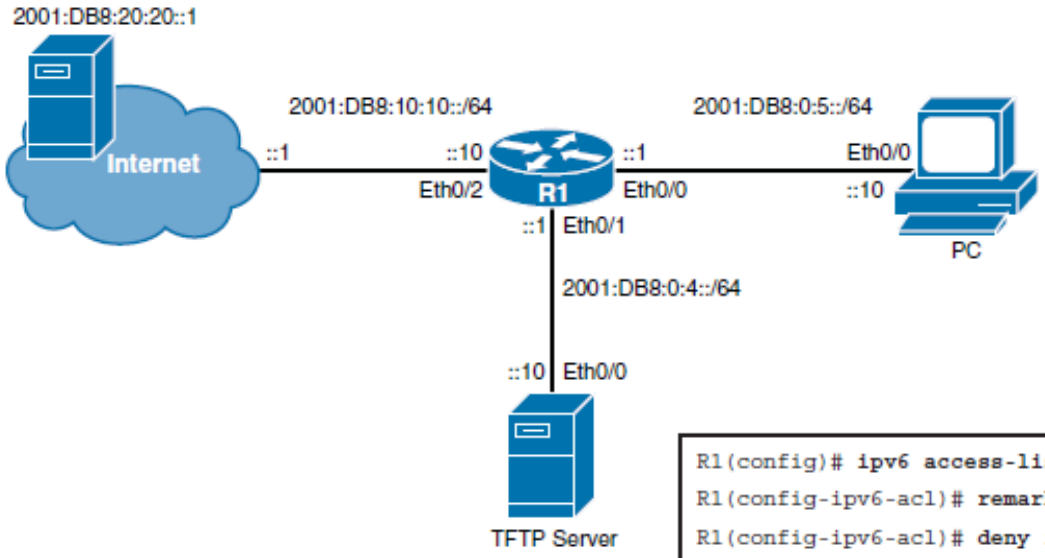
NPTv6

- NPTv6 is described in RFC 6296, *IPv6-to-IPv6 Network Prefix Translation* . (Note that at the time of this writing this RFC has an "experimental," not "standard," status.)
- NPTv6 is a one-to-one stateless translation; one IPv6 address in an inside network, such as an organization's LAN, is translated to one IPv6 address in an outside network, the IPv6 Internet.

# IPv6 ACLs

- One change from IPv4 is that IPv6 ACLs are always named and extended.
- For IPv6, there are three implicit rules at the end of each ACL, as follows:
  - `permit icmp any any nd-na`
  - `permit icmp any any nd-ns`
  - `deny ipv6 any any`
- If you want to log all packets that are denied, simply add a **deny ipv6 any any log** command to your ACL.
- However, this explicit **deny** command would override all three implicit rules, you would need to explicitly configure the two **permit nd** statements, followed by the explicit **deny** statement.

# Configuring IPv6 ACLs




```
R1(config)# ipv6 access-list SECURE_HOSTS
R1(config-ipv6-acl)# remark DENY PING TO TFTP SERVER
R1(config-ipv6-acl)# deny icmp any host 2001:DB8:0:4::10 echo-request
R1(config-ipv6-acl)# remark DENY TELNET TO TFTP SERVER
R1(config-ipv6-acl)# deny tcp any host 2001:DB8:0:4::10 eq telnet
R1(config-ipv6-acl)# remark ALLOW TFTP ONLY TO TFTP SERVER
R1(config-ipv6-acl)# permit udp any host 2001:DB8:0:4::10 eq tftp
R1(config-ipv6-acl)# deny udp any any eq tftp
R1(config-ipv6-acl)# remark ALLOW ALL OTHER TRAFFIC
R1(config-ipv6-acl)# permit ipv6 any any
```

```
R1(config)# interface Ethernet 0/2
R1(config-if)# ipv6 traffic-filter SECURE_HOSTS in
```

# Verifying IPv6 ACLs

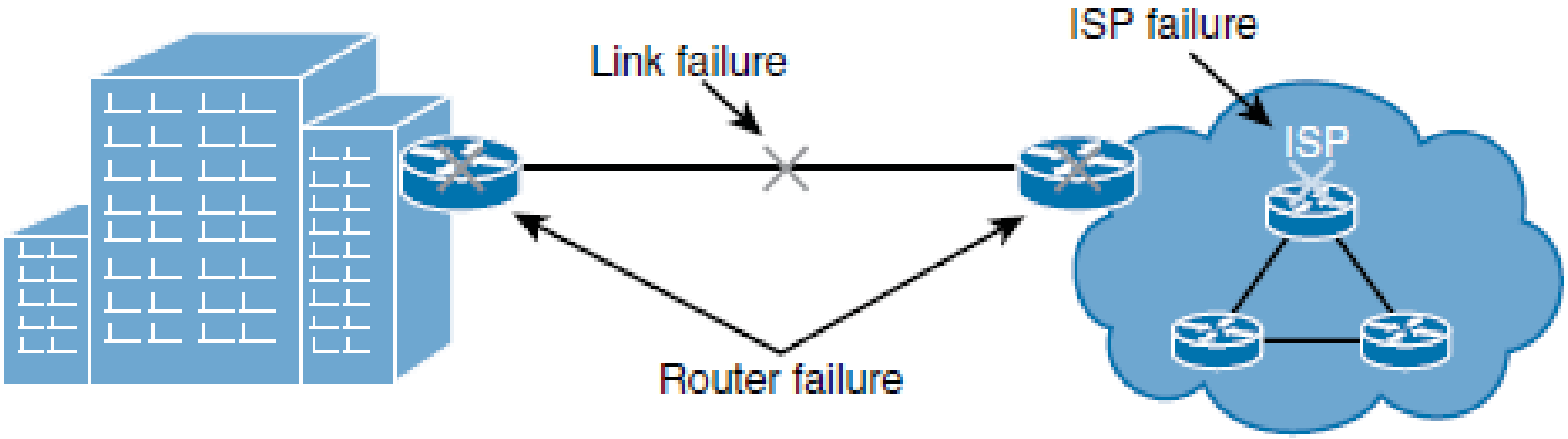
```
R1# show ipv6 access-list
IPv6 access list SECURE_HOSTS
    deny icmp any host 2001:DB8:0:4::10 echo-request (5 matches) sequence 20
    deny tcp any host 2001:DB8:0:4::10 eq telnet (1 match) sequence 40
    permit udp any host 2001:DB8:0:4::10 eq tftp (4 matches) sequence 60
    deny udp any any eq tftp (6 matches) sequence 70
    permit ipv6 any any (44 matches) sequence 90
```

# Improving Internet Connectivity Resilience

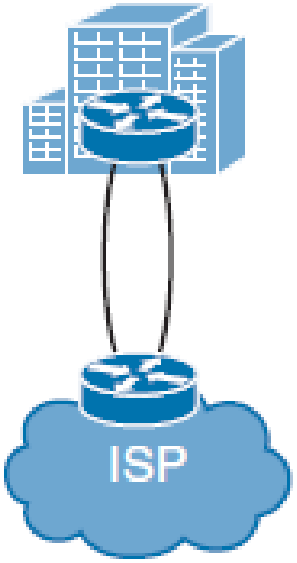
# Improving Internet Connectivity Resilience

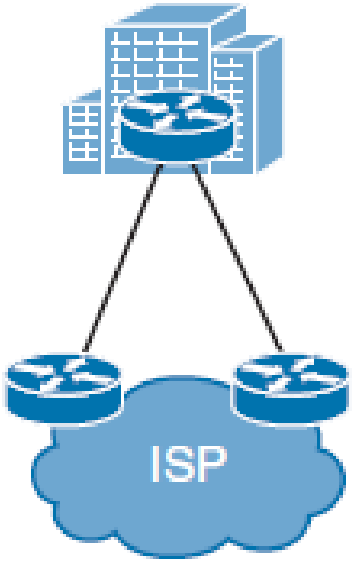
- Describe the disadvantages of single-homed Internet connectivity
- Describe dual-homed Internet connectivity
- Describe multihomed Internet connectivity

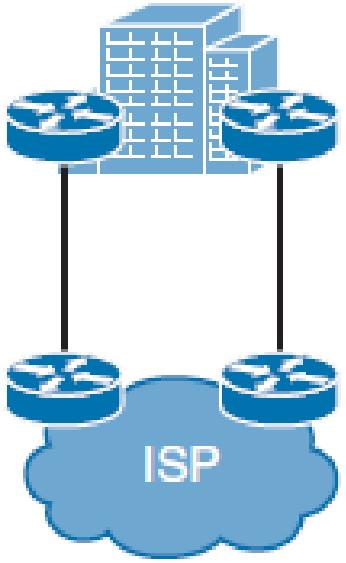
# Drawbacks of a Single-Homed Internet Connectivity



# Dual-Homed Internet Connectivity



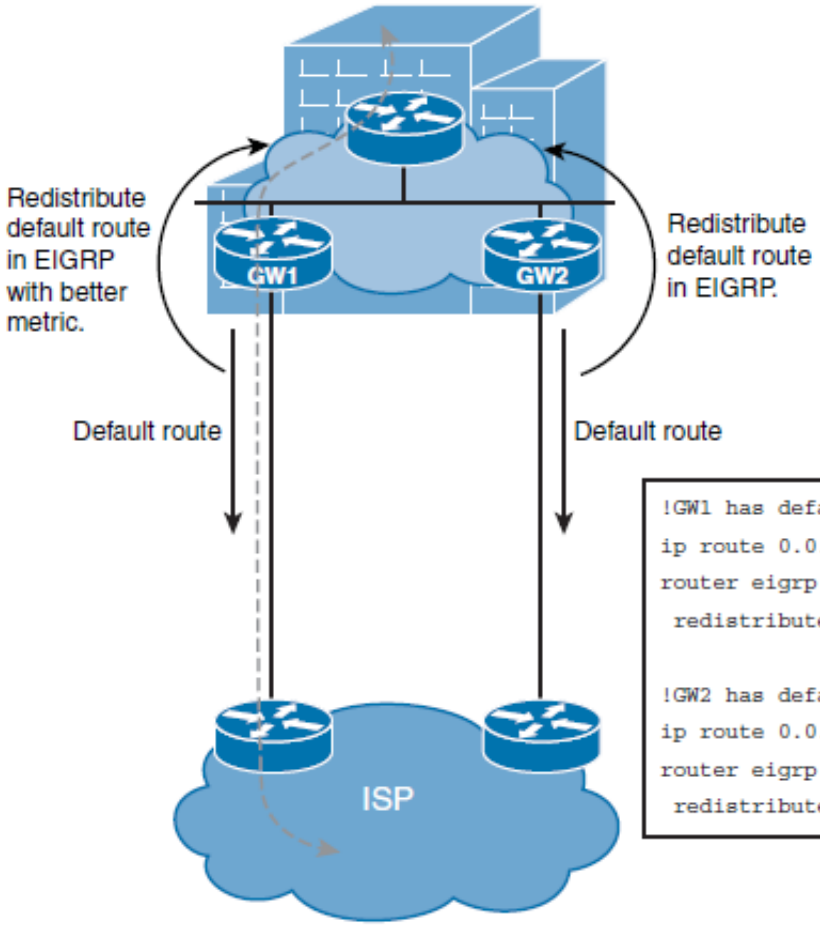



# Configuring Best Path for Dual-Homed Internet Connectivity

- In dual-homed networks, one link is usually used as a primary link. In case of primary link failure, the second (backup) link is used for traffic forwarding.
- Either static routing toward the ISP or BGP with the ISP are commonly used to route outbound traffic.
- Internet routing information must also be available to the organization's internal routing protocol. In simple networks, static routes with different ADs (called floating static routes) can be used.
- Alternatively, you can redistribute a default route or a subset of Internet routes into your internal routing protocol.
- First-hop redundancy protocols (FHRPs) can also be used to properly route packets to the appropriate Internet gateway.

# Dual-Homed EIGRP and Static Example

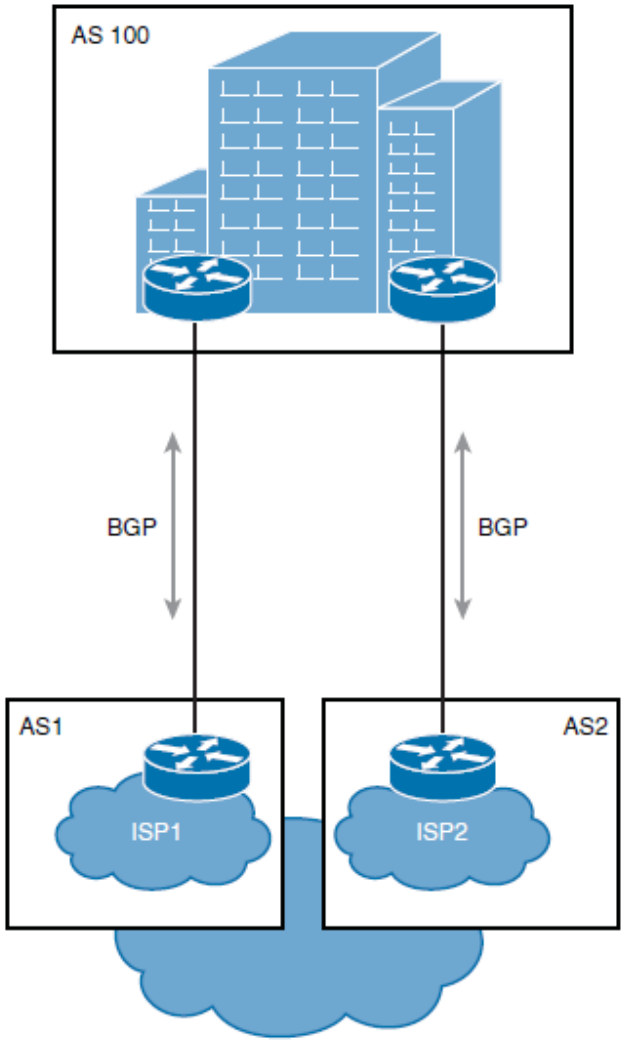



```
!GW1 has default route to one ISP router
ip route 0.0.0.0 0.0.0.0 209.165.201.129
router eigrp 1
 redistribute static metric 20000 1 255 1 1500

!GW2 has default route to the other ISP router
ip route 0.0.0.0 0.0.0.0 209.165.202.129
router eigrp 1
 redistribute static metric 10000 1 255 1 1500
```

# Multihomed Internet Connectivity

- The multihomed Internet design offers the highest level of redundancy. It resolves all single points of failure issues and provides a reliable link to the Internet.
- Two routers are commonly used as Internet gateways, and each router is connected to a different ISP using one or more physical links.

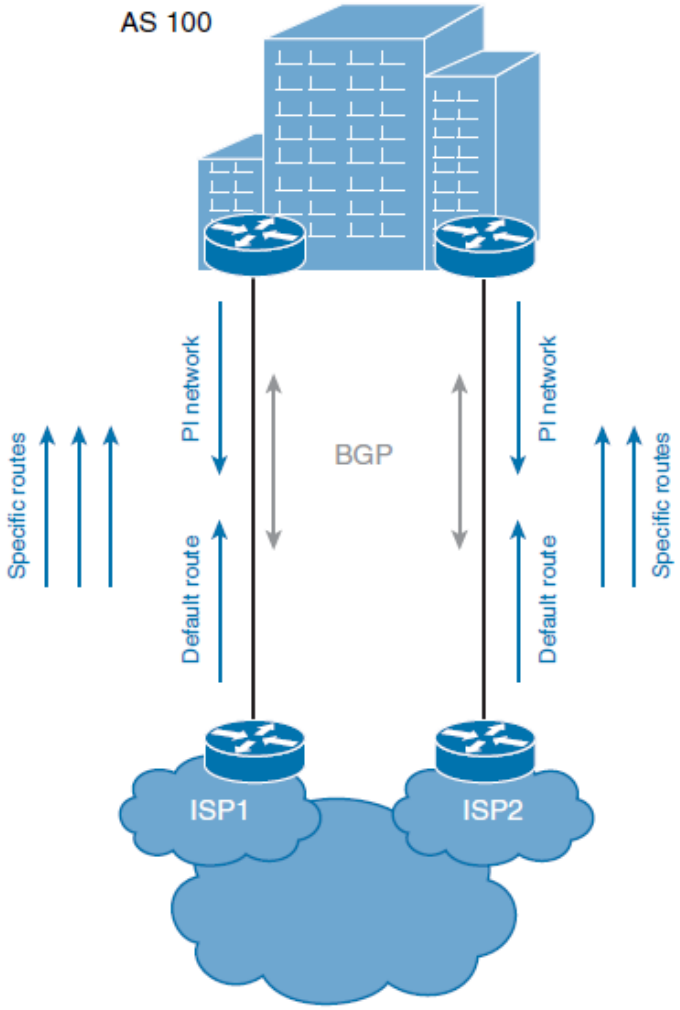


# Multihomed Internet Connectivity

- Establishing a multihomed environment involves meeting some requirements:
  - You must have PI (Provider Independent) address space and your own autonomous system number.
  - You must establish connectivity with two independent ISPs.

# Options for Routes That ISPs in a Multihomed Design Can Send

- The ISPs can send the following to your network:
  - The ISPs can send only a default route.
  - The ISPs can send a partial routing table and a default route.
  - The ISPs could also send you a full routing table.



# Chapter 6 Summary

- Internet connectivity requirements: outbound only, or also inbound.
- Internet connectivity redundancy options: edge device, link, and ISP.
- The four connection redundancy types:
  - **Single-homed:** One connection to one ISP
  - **Dual-homed:** Two connections to one ISP
  - **Multihomed:** One connection to each of multiple (usually two) ISPs
  - **Dual multihomed:** Two connections to each of two ISPs
- Public IP address assignment: The IANA assigns to RIRs; RIRs assign to ISPs and organizations.

# Chapter 6 Summary

- IP addresses, which can be PI or PA.
- Routing protocols that are either IGPs (and operate within an autonomous system) or EGPs (and operate between autonomous systems). BGP is the protocol used between autonomous systems on the Internet.
- The range of private autonomous system numbers: 64,512 to 65,534 and 4,200,000,000 through 4,294,967,294 (64,086.59904 through 65,535.65534).
- Provider-assigned IPv4 addresses, which can be configured statically or via DHCP.
- DHCPv4 operation, including the DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK messages.
- The use of NAT for IPv4, typically to translate private addresses to public addresses.

# Chapter 6 Summary

- The four types of NAT addresses:
  - **Inside local address:** The IPv4 address assigned to a device on the internal network.
  - **Inside global address:** The IPv4 address of an internal device as it appears to the external network. This is the address to which the inside local address is translated.
  - **Outside local address:** The IPv4 address of an external device as it appears to the internal network. If outside addresses are being translated, this is the address to which the outside global address is translated.
  - **Outside global address:** The IPv4 address assigned to a device on the external network.
- The three types of NAT: static (one-to-one), dynamic (many-to-many), and PAT (many-to-one).
- The order of operations for NAT: It first performs routing and then translation when going from an inside interface to an outside interface, and vice versa when the traffic flow is reversed.

# Chapter 6 Summary

- NAT issues, including when an inside device tries to communicate with a device on another inside interface.
- NVI, which removes the requirement to configure an interface as inside or outside. NVI also operates differently; it performs routing, translation, and routing again. The whole process is symmetrical, no matter which way the traffic is flowing.
- Configuring a Cisco router to be a DHCP server and a DHCP relay agent, for both IPv4 and IPv6.
- IPv6 addresses, which can be configured with the following methods:
  - Manual Assignment
  - SLAAC
  - Stateless DHCPv6
  - Stateful DHCPv6
  - DHCPv6-PD

# Chapter 6 Summary

- DHCPv6 operation, including the SOLICIT, ADVERTISE, REQUEST, and REPLY messages.
- Two types of NAT for IPv6: NAT64 and NPTv6.
- IPv6 ACLs, which include three implicit rules at the end of each ACL, as follows:
  - **permit icmp any any nd-na**
  - **permit icmp any any nd-ns**
  - **deny ipv6 any any**
- Applying an IPv6 ACL to an interface, using the **ipv6 traffic-filter** *ACL-name* { **in|out** } interface configuration command. Notice the **traffic-filter** keyword is used rather than the **access-group** keyword that is used in IPv4 ACLs.
- The need to secure devices connected to the IPv6 Internet.
- The drawbacks of single-homed Internet connectivity because of the single points of failure: link failure, ISP failure, or router failure.

# Chapter 6 Summary

- Using a dual-homed design to improve redundancy: two (or more) connections, using one or more Internet routers, to the same ISP. The ISP may also have multiple routers to connect to specific customers. Static routes or BGP are used. One link can be primary, or traffic can be load balanced over both links.
- Using a multihomed design to further improve redundancy; two routers are used as Internet gateways, and each router is connected to a different ISP using one or more physical links.
- The options for what ISPs can send to your network in a multihomed design:
  - Only a default route
  - A partial routing table (of a subset of routes originated near the ISP) and a default route
  - A full routing table
- How receiving full routing tables consume a lot of router resources.

# Chapter 6 Labs

- **CCNPv7 ROUTE Lab6.1 NAT**

# Acknowledgment


- Some of images and texts are from Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide by Diane Teare, Bob Vachon and Rick Graziani (1587204568)



- Special Thanks to *Bruno Silva*