RADFORD UNIVERSITY

Internet Routing Protocols, DHCP, and NAT

Hwajung Lee

Modified from Slides Courtesy of
Cisco Networking Academy and
the book titled Communication Networks by Leon-Garcia

Contents

- Basic Routing
- Single Area Open Shortest Path First (OSPF)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)
- Summary

Autonomous Systems

- Global Internet viewed as collection of autonomous systems.
- **Autonomous system (AS)** is a set of routers or networks administered by a single organization
- Same routing protocol need not be run within the AS
- But, to the outside world, an AS should present a *consistent picture of what ASs are reachable* through it
- **Stub AS:** has only a single connection to the outside world.
- **Multihomed AS:** has multiple connections to the outside world, but refuses to carry transit traffic
- **Transit AS:** has multiple connections to the outside world, and can carry transit and local traffic.

AS Number

- For exterior routing, an AS needs a globally unique AS 16-bit integer number
- *Stub AS*, which is the most common type, does not need an AS number since the prefixes are placed at the provider's routing table
- *Transit AS* needs an AS number
- Request an AS number from one of the five RIRs (Regional Internet Registries)
  - ARIN: American Registry for Internet Numbers
  - RIPE NCC: Réseaux IP Européens Network Coordination Centre
  - APNIC: Asia Pacific Network Information Centre
  - LACNIC: Latin America and Caribbean Network Information Centre
  - AFRINIC: African Network Information Centre

Inter and Intra Domain Routing

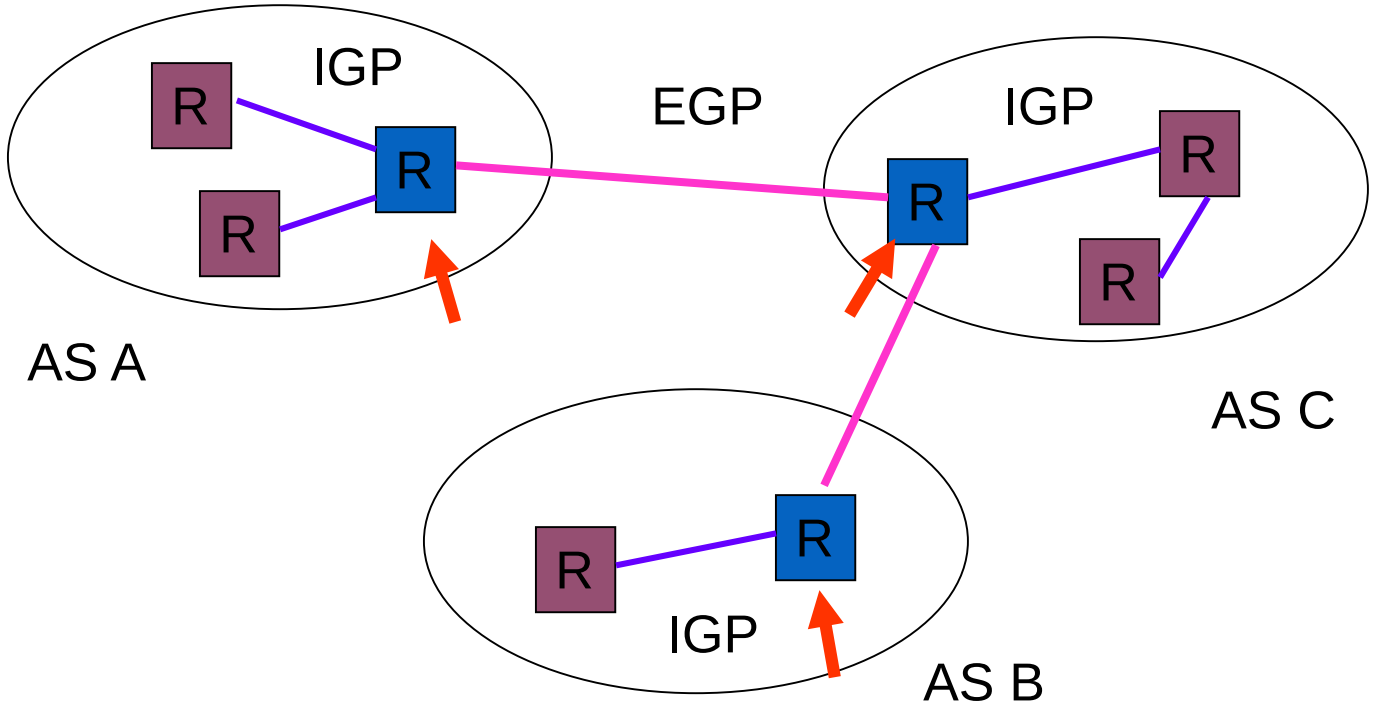
Interior Gateway Protocol (IGP): routing within AS

- RIP, OSPF, IGRP, EIGRP, IS-IS

Exterior Gateway Protocol (EGP): routing between AS's

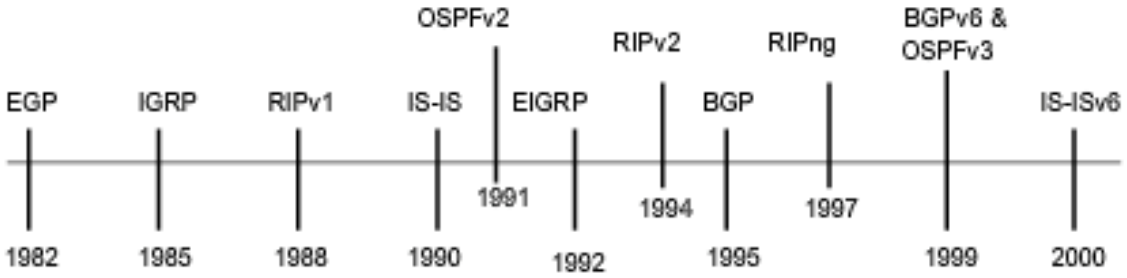
- BGPv4

Border Gateways perform IGP & EGP routing



Inter and Intra Domain Routing

Routing Protocols Evolution and Classification

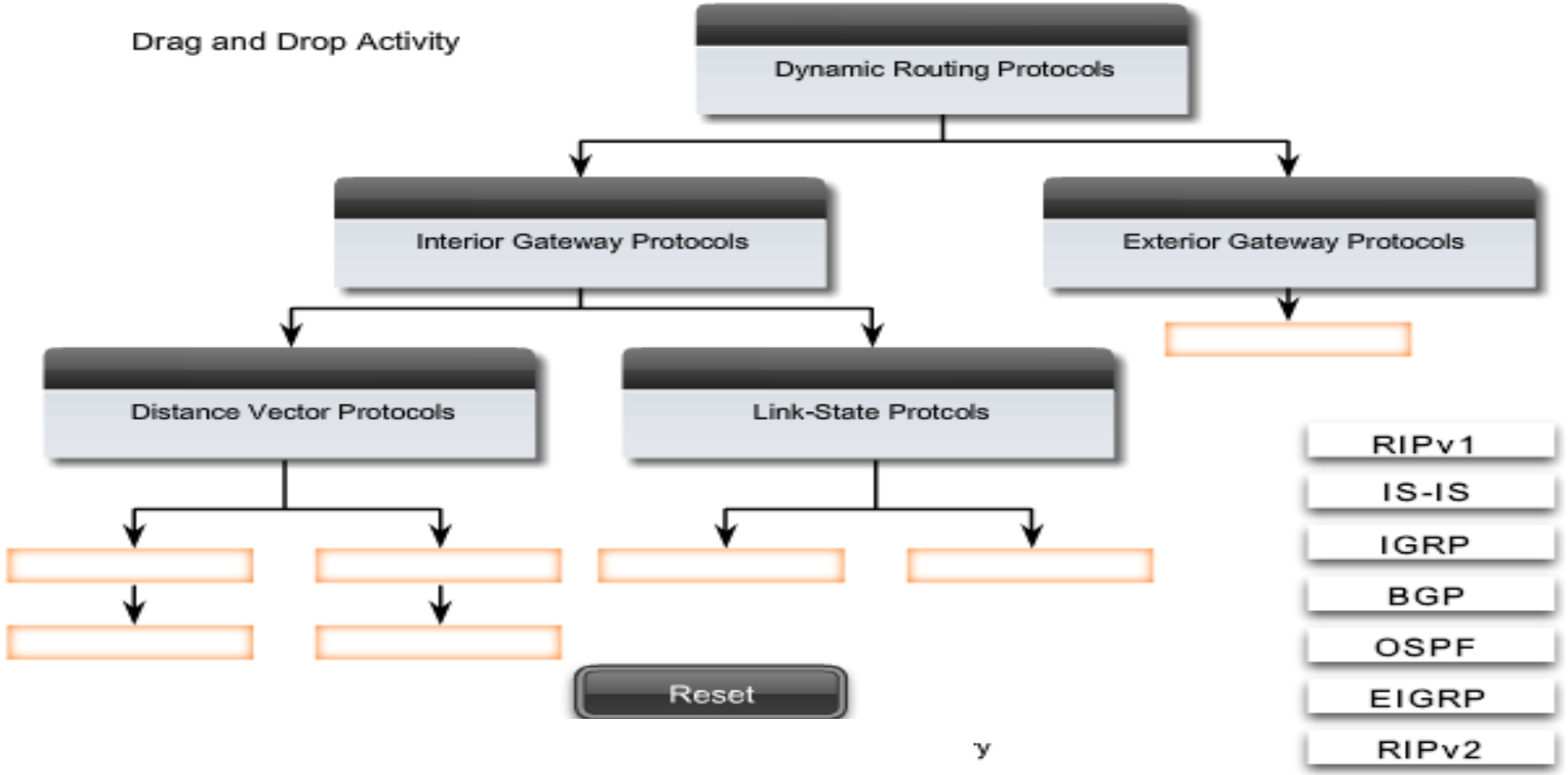


	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector Routing Protocols		Link State Routing Protocols		Path Vector
Classful	RIP	IGRP			EGP
Classless	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGPv4 for IPv6

Highlighted routing protocols are the focus of this course.

Image Source: www.netacad.com

Inter and Intra Domain Routing



Open Shortest Path First

- RFC 2328 (v2)
- Fixes some of the deficiencies in RIP
- Enables each router to learn complete network topology
- Each router monitors the *link state* to each neighbor and floods the link-state information to other routers
- Each router builds an identical *link-state database*
- Allows router to build shortest path tree with router as root
- OSPF typically converges faster than RIP when there is a failure in the network

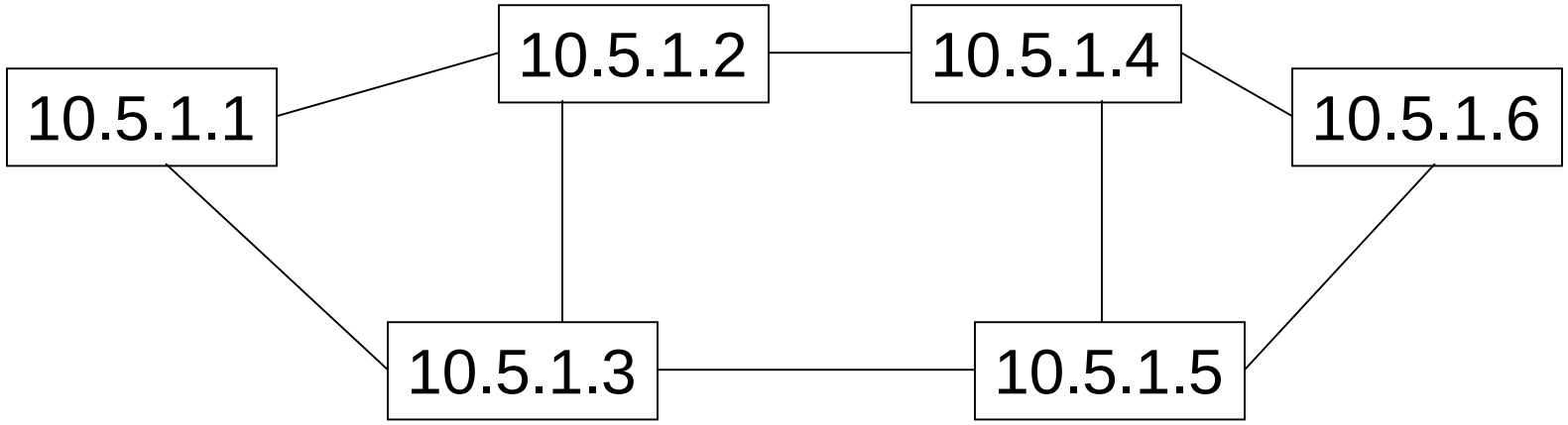
OSPF Features

- *Multiple routes* to a given destination, one per type of service
- Support for *variable-length subnetting* by including the subnet mask in the routing message
- Distribution of traffic over *multiple paths* of equal cost
- Uses *notion of area* to partition sites into subsets
- Support *host-specific routes* as well as net-specific routes
- *Designated router* to minimize table maintenance overhead

Flooding

- Used in OSPF to distribute link state (LS) information
- Forward incoming packet to all ports except where packet came in
- Packet eventually reaches destination as long as there is a path between the source and destination
- Generates exponential number of packet transmissions
- Approaches to limit # of transmissions:
  - Use a TTL at each packet; won't flood if TTL is reached
  - Each router adds its identifier to header of packet before it floods the packet; won't flood if its identifier is detected
  - Each packet from a given source is identified with a unique sequence number; won't flood if sequence number is same

Example OSPF Topology



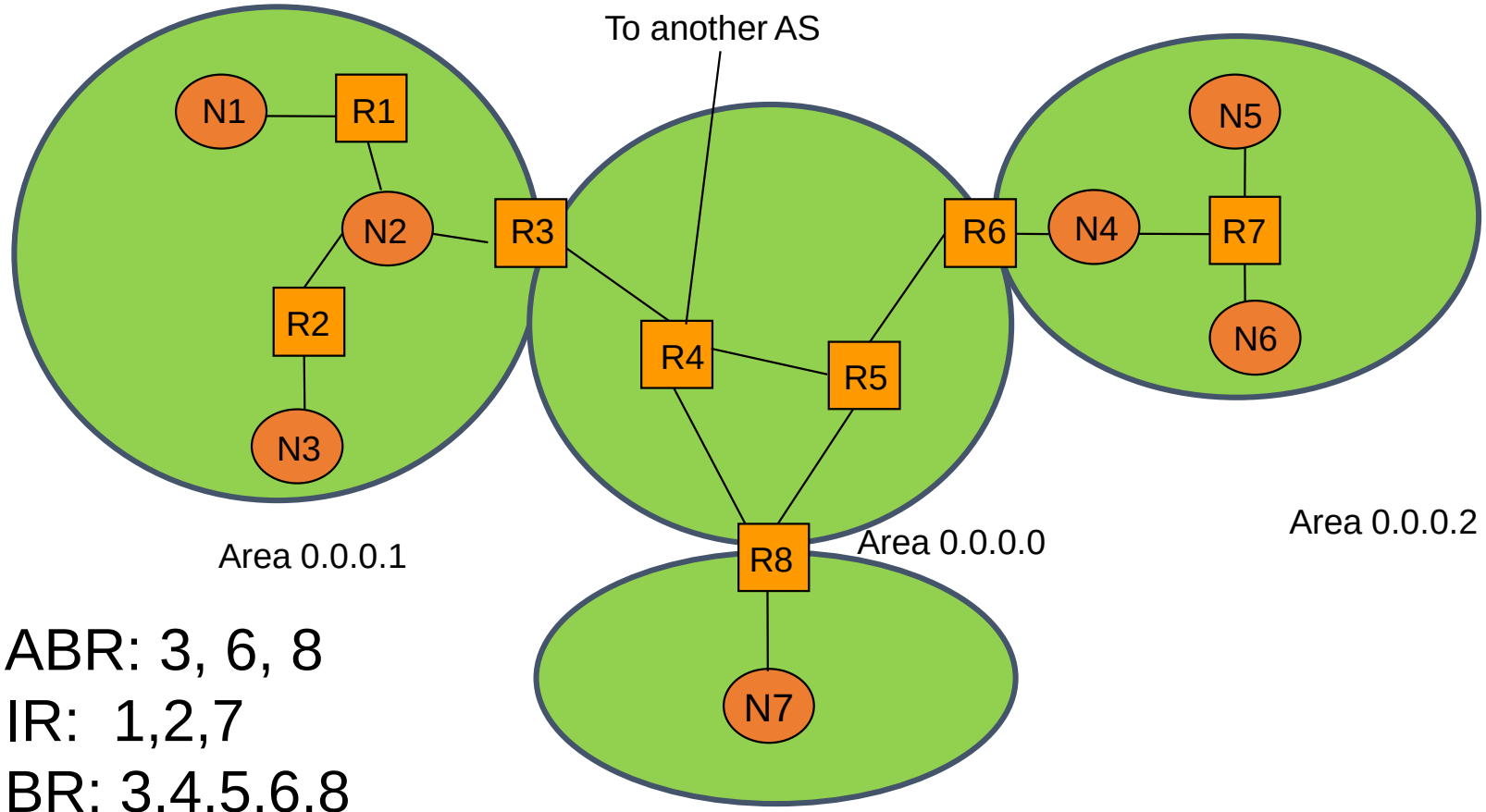
At steady state:

- All routers have same LS database
- Know how many routers in network
- Interfaces & links between routers
- Cost of each link
- Occasional Hello messages (10 sec) & LS updates sent (30 min)

OSPF Network

- To improve scalability, AS may be partitioned into *areas*
  - Area is identified by 32-bit Area ID
  - Router in area only knows complete topology inside area & limits the flooding of link-state information to area
  - *Area border routers* summarize info from other areas
- Each area must be connected to *backbone area* (0.0.0.0)
  - Distributes routing info between areas
- *Internal router* has all links to nets within the same area
- *Area border router* has links to more than one area
- *Backbone router* has links connected to the backbone

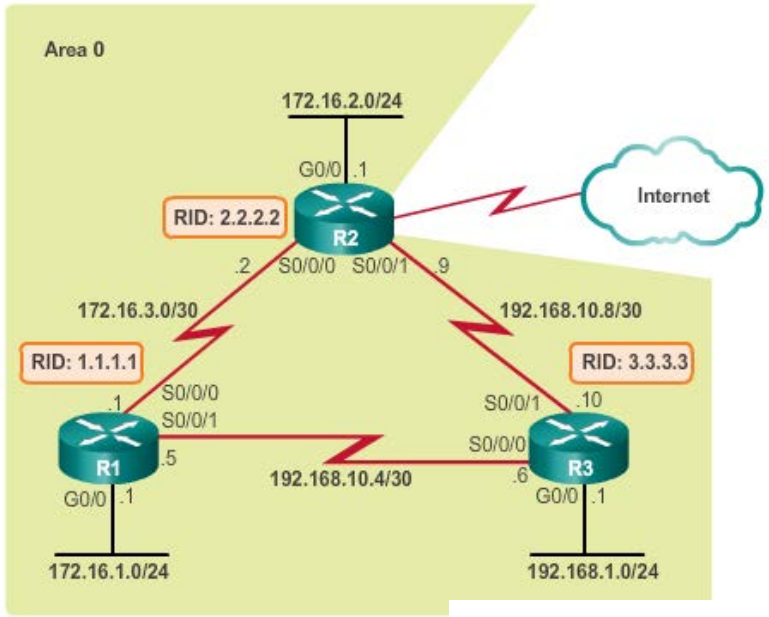
OSPF Areas



ABR: 3, 6, 8
IR: 1,2,7
BR: 3,4,5,6,8

R = router
N = network

Configuring Single-Area OSPF




```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
R1(config-router)# passive-interface g0/0
R1(config-router)#
```

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# exit
R2(config)# router ospf 10
R2(config-router)# router-id 2.2.2.2
R2(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R2(config-router)# network 172.16.2.1 0.0.0.0 area 0
R2(config-router)# network 172.16.3.2 0.0.0.0 area 0
R2(config-router)# network 192.168.10.9 0.0.0.0 area 0
R2(config-router)#
R2(config-router)# passive-interface g0/0
R2(config-router)#
```

Verifying Single-Area OSPF

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:32    192.168.10.6    Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:38    172.16.3.2      Serial0/0/0
R1#
```

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    172.16.3.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:12:14
    2.2.2.2              110      00:12:46
  Distance: (default is 110)

R1#v
```

Verifying Single-Area OSPF (cont.)

```
R1# show ip ospf
 Routing Process "ospf 10" with ID 1.1.1.1
 Start time: 00:06:18.952, Time elapsed: 00:39:56.400

 <Output omitted>

 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 1000 mbps
 Area BACKBONE(0)
        Number of interfaces in this area is 3
Area has no authentication
SPF algorithm last executed 00:15:21.436 ago
SPF algorithm executed 6 times
Area ranges are
Number of LSA 3. Checksum Sum 0x023523
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

R1#
```

Verifying Single-Area OSPF (cont.)

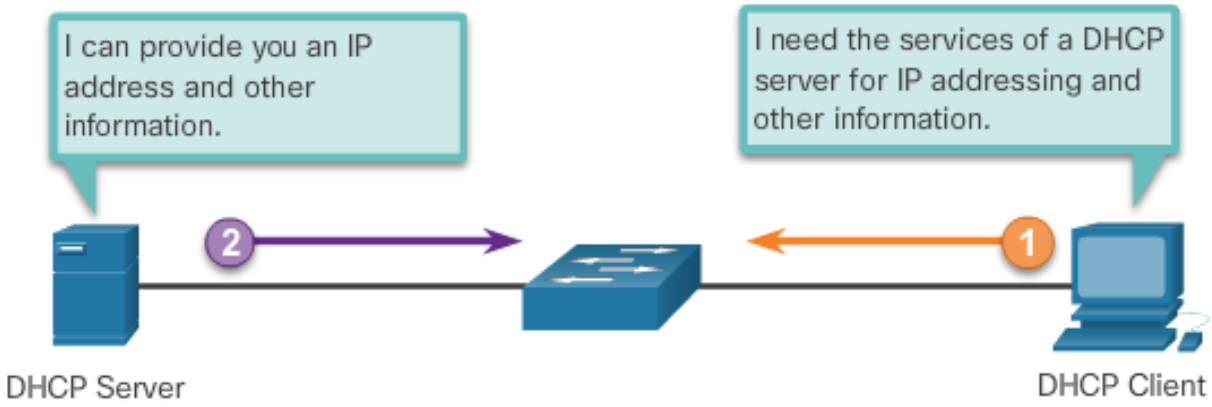
```
R1# show ip ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.1.1/24, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 172.16.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.10.5/30, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT,
Cost: 647

 <Output omitted>
```

```
R1# show ip ospf interface brief
Interface    PID   Area    IP Address/Mask    Cost  State Nbrs F/C
Gi0/0        10    0       172.16.1.1/24      1     DR    0/0
Se0/0/1      10    0       192.168.10.5/30    647   P2P   1/1
Se0/0/0      10    0       172.16.3.1/30      647   P2P   1/1
R1#
```

Introducing DHCPv4

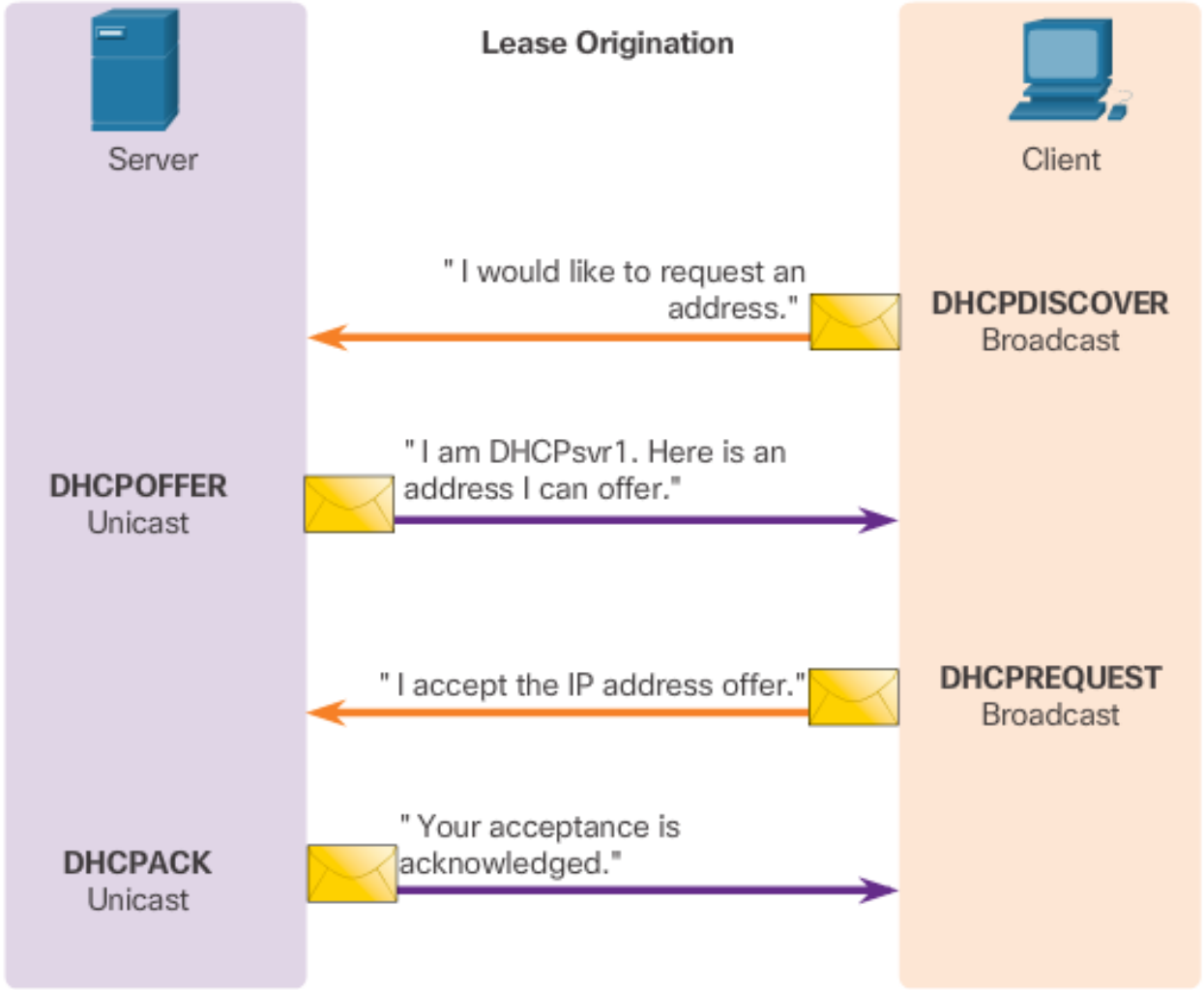
- DHCPv4:
  - assigns IPv4 addresses and other network configuration information dynamically
  - useful and timesaving tool for network administrators
  - dynamically assigns, or leases, an IPv4 address from a pool of addresses
- A Cisco router can be configured to provide DHCPv4 services.
- Administrators configure DHCPv4 servers so that leases expire. Then the client must ask for another address, although the client is typically reassigned the same address.



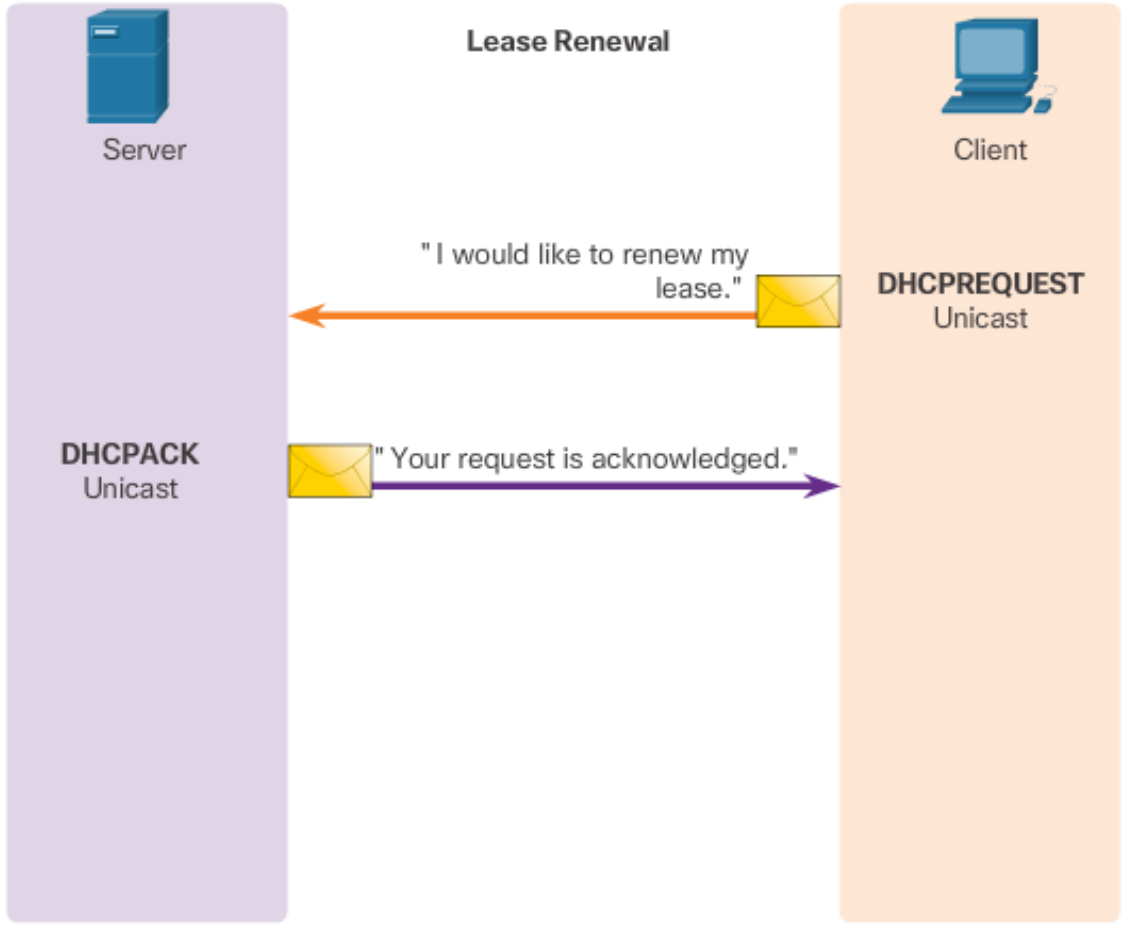
DHCP Operation

- Host broadcasts DHCP *Discover* message on its physical network
- Server replies with *Offer* message (IP address + configuration information)
- Host selects one offer and broadcasts *DHCP Request* message
- Server allocates IP address for lease time T
  - Sends DHCP ACK message with T, and threshold times T1 (=1/2 T) and T2 (=.875T)
- At T1, host attempts to renew lease by sending DHCP Request message to original server
- If no reply by T2, host broadcasts DHCP Request to *any* server
- If no reply by T, host must relinquish IP address and start from the beginning

DHCPv4 Operation



DHCPv4 Operation (cont.)

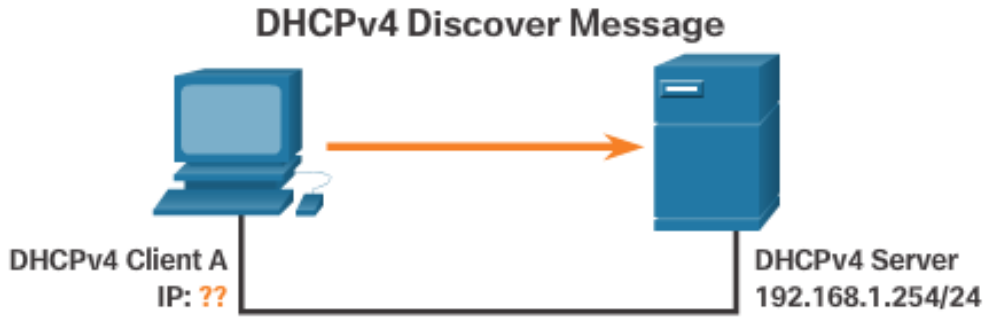


DHCPv4 Message Format

8	16	24	32
OP Code (1)	Hardware Type (1)	Hardware Address Length (1)	Hops (1)
Transaction Identifier			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Boot Filename - 128 bytes			
DHCP Options - variable			

DHCPv4 Operation

DHCPv4 Discover and Offer Messages

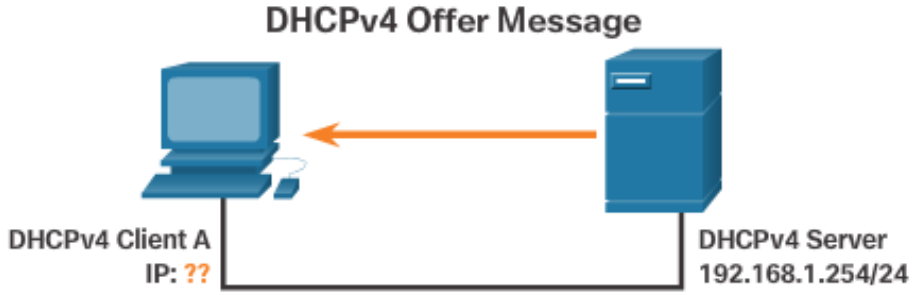


Ethernet Frame	IP	UDP	DHCPDISCOVER
DST MAC: FF:FF:FF:FF:FF:FF SRC MAC: MAC A	IP SRC: 0.0.0.0 IP DST: 255.255.255.255	UDP 67	CIADDR: 0.0.0.0 GIADDR: 0.0.0.0 Mask: 0.0.0.0 CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

The DHCP client sends an IP broadcast with a DHCPDISCOVER packet. In this example, the DHCP server is on the same segment and will pick up this request. The server notes the GIADDR field is blank; therefore, the client is on the same segment. The server also notes the hardware address of the client in the request packet.

DHCPv4 Discover and Offer Messages (cont.)



Ethernet Frame	IP	UDP	DHCP Reply
DST MAC: MAC A SRC MAC: MAC Serv	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 GIADDR: 0.0.0.0 Mask: 255.255.255.0 CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

The DHCP server picks an IP address from the available pool for that segment, as well as the other segment and global parameters. The DHCP server puts them into the appropriate fields of the DHCP packet. The DHCP server then uses the hardware address of A (in CHADDR) to construct an appropriate frame to send back to the

Configure a Basic DHCPv4 Server

A Cisco router running the Cisco IOS software can be configured to act as a DHCPv4 server. To set up DHCP:

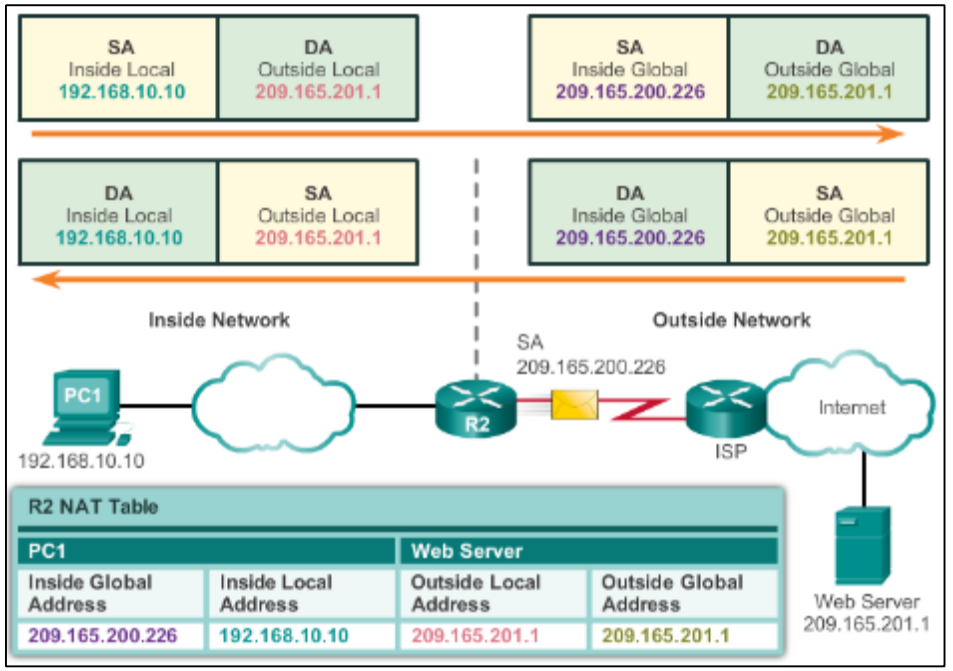
1. Exclude addresses from the pool.
2. Set up the DHCP pool name.
3. Define the range of addresses and subnet mask. Use the **`default-router`** command for the default gateway. Optional parameters that can be included in the *pool – dns server*, *domain-name*.

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

To disable DHCP, use the **no service dhcp** command.

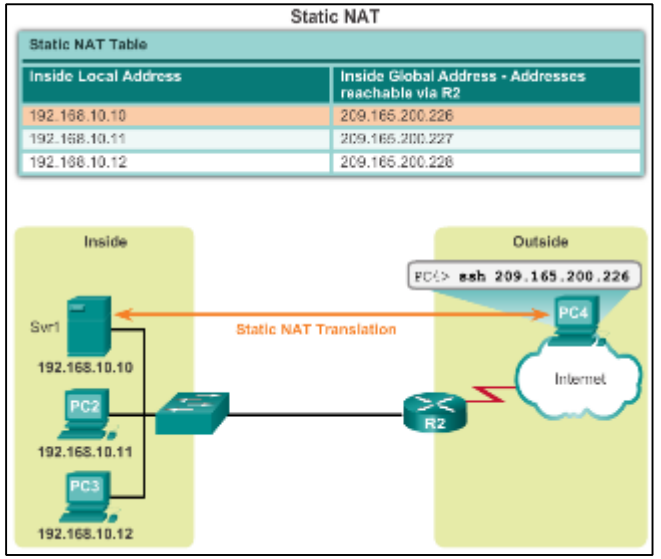
NAT Characteristics

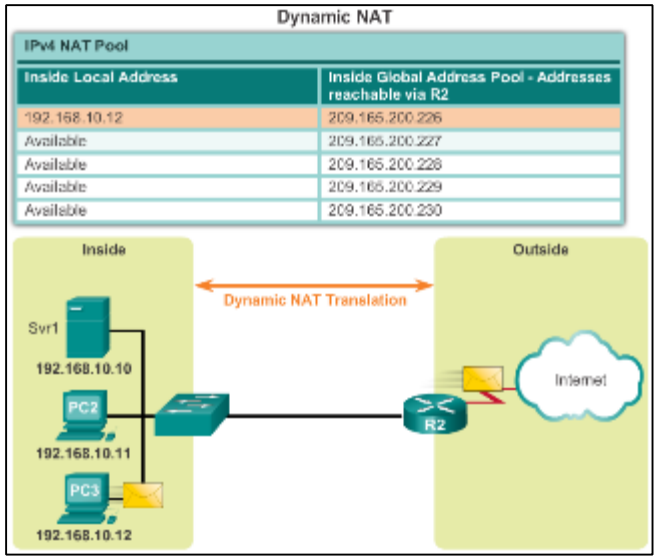
- IPv4 Private Address Space
  - 10.0.0.0 /8, 172.16.0.0 /12, and 192.168.0.0 /16
- What is NAT?
  - Process to translate network IPv4 address
  - Conserve public IPv4 addresses
  - Configured at the border router for translation
- NAT Terminology
  - Inside address
  - Inside local address
  - Inside global address
  - Outside address
  - Outside local address
  - Outside global address



Types of NAT

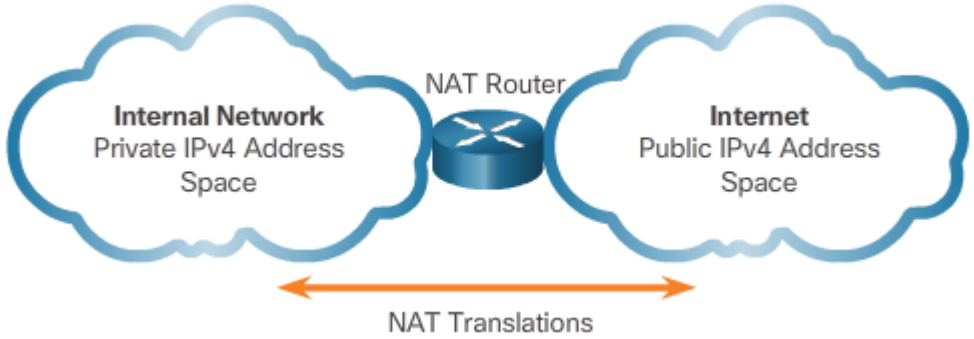
- Static NAT
  - One-to-one mapping of local and global addresses
  - Configured by the network administrator and remain constant.
- Dynamic NAT
  - Uses a pool of public addresses and assigns them on a first-come, first-served basis
  - Requires that enough public addresses for the total number of simultaneous user sessions
- Port Address Translation (PAT)
  - Maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses
  - Also known as NAT overload
  - Validates that the incoming packets were requested
  - Uses port numbers to forward the response packets to the correct internal device





NAT Advantages

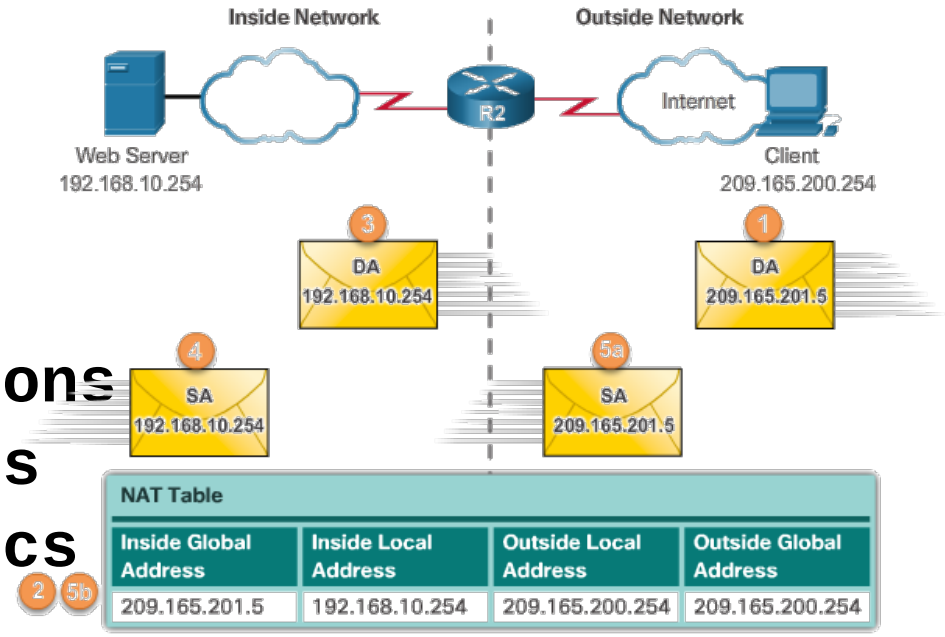
- Advantages of NAT
  - Conserves the legally registered addressing scheme
  - Increases the flexibility of connections to the public network
  - Provides consistency for internal network addressing schemes
  - Provides network security
- Disadvantages of NAT
  - Performance is degraded
  - End-to-end functionality is degraded
  - End-to-end IP traceability is lost
  - Tunneling is more complicated
  - Initiating TCP connections can be disrupted



Configuring Static NAT

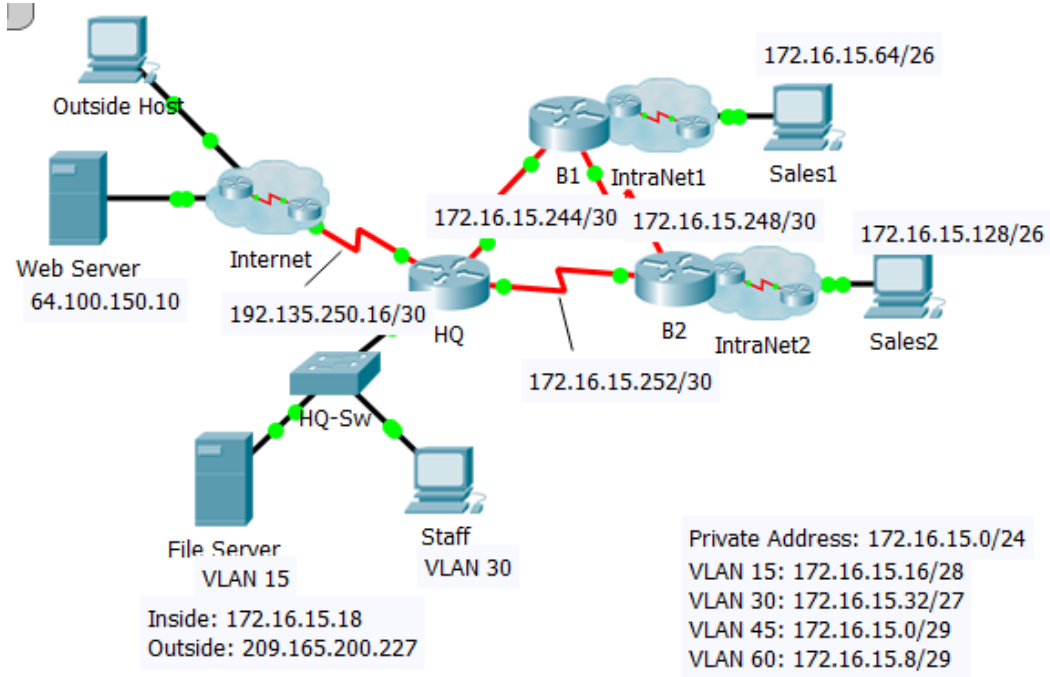
- Configuring Static NAT
  - Create the mapping between the inside local and outside local addresses
    - **`ip nat inside source static`** *`local-ip global-ip`*
  - Define which interfaces belong to the inside network and which belong to the outside network
    - **`ip nat inside`**
    - **`ip nat outside`**
- Analyzing Static NAT
- Verifying Static NAT

  `show ip nat translations`
  `show ip nat statistics`
  `clear ip nat statistics`



NAT – Sample Configuration

```
access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
[ip nat inside source list 1 s 0/1/0 overload]
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
   ip nat inside
interface s0/0/1
   ip nat inside
interface s0/1/0
   ip nat outside
```



Configuring Dynamic NAT

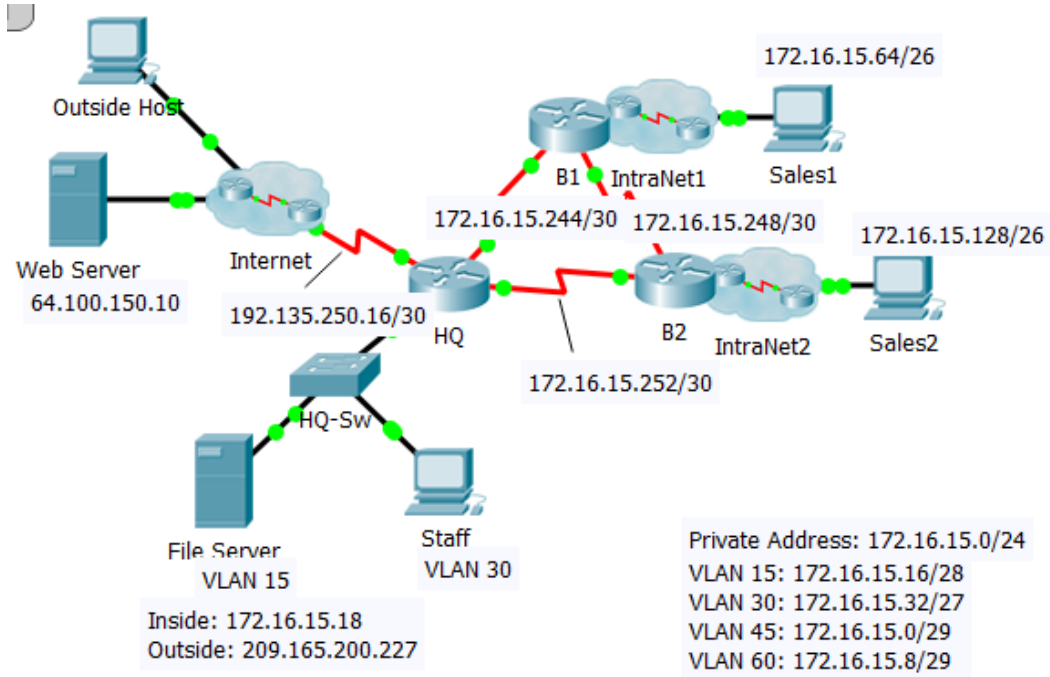
- Dynamic NAT Operation
  - The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come, first-served basis.
  - With dynamic NAT, a single inside address is translated to a single outside address.
  - The pool must be large enough to accommodate all inside devices.
  - A device is unable to communicate to any external networks if no addresses are available in the pool.

Configuring Dynamic NAT (Cont.)

- Configuring Dynamic NAT
  - Create the mapping between the inside local and outside local addresses
    - **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
  - Create a standard ACL to permit those addresses to be translated
    - **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
  - Bind the ACL to the pool
    - **ip nat inside source list** *access-list-number* **pool** *name*
  - Identify the inside and outside interfaces
    - **ip nat inside**
    - **ip nat outside**

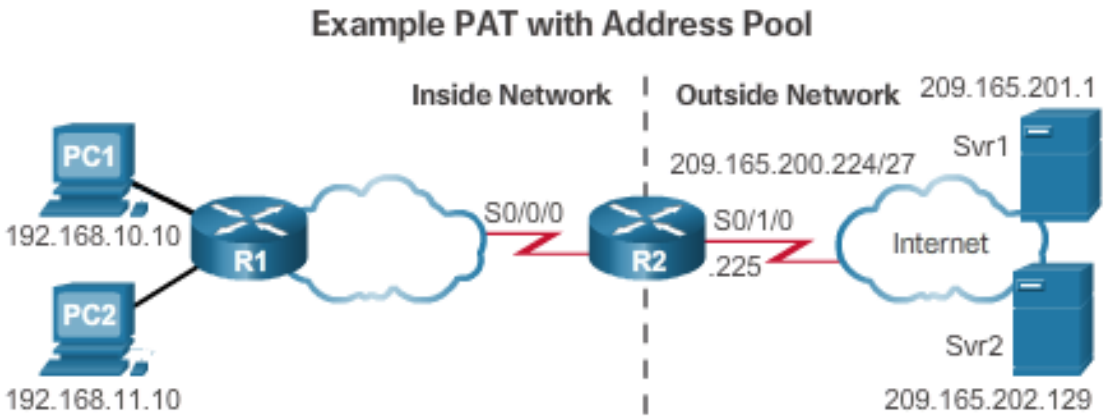
NAT – Sample Configuration

```
access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
   ip nat inside
interface s0/0/1
   ip nat inside
interface s0/1/0
   ip nat outside
```



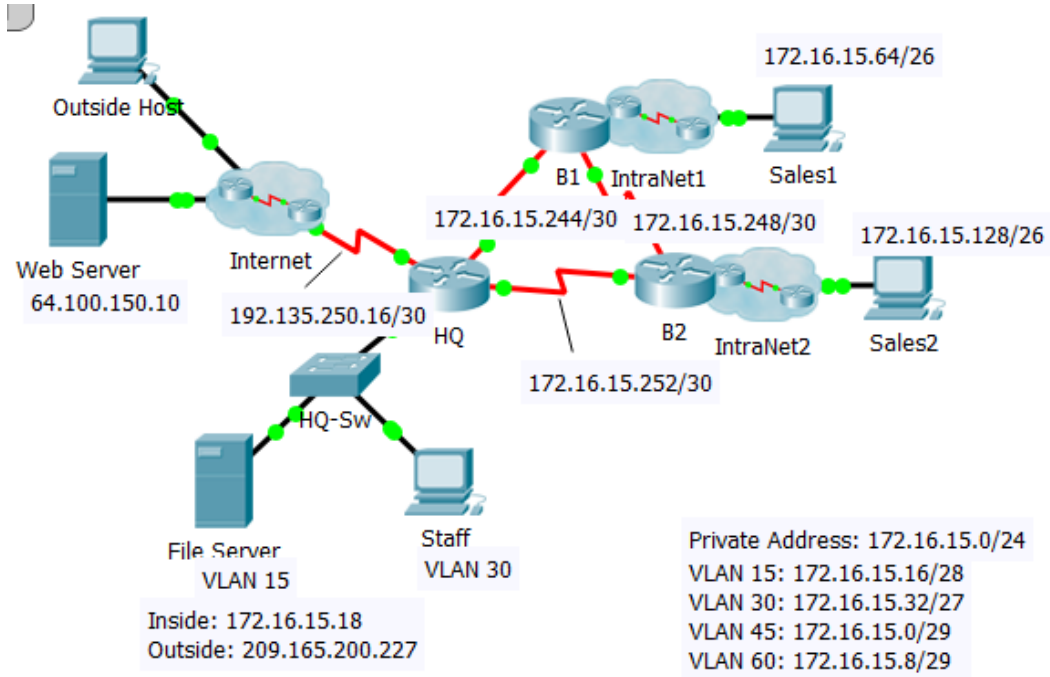
Configuring Port Address Translations (PAT)

- Configuring PAT: Address Pool
  - Create the mapping between the inside local and outside local addresses
    - **`ip nat pool name`** *`start-ip end-ip`* {**`netmask`** *`netmask`* | **`prefix-length`** *`prefix-length`*}
  - Create a standard ACL to permit those addresses to be translated
    - **`access-list`** *`access-list-number`* **`permit`** *`source`* [*`source-wildcard`*]
  - Bind the ACL to the pool
    - **`ip nat inside source list`** ***`access-list-number`*** **`pool`** ***`name overload`***
  - Identify the inside and outside interfaces
    - **`ip nat inside`**
    - **`ip nat outside`**



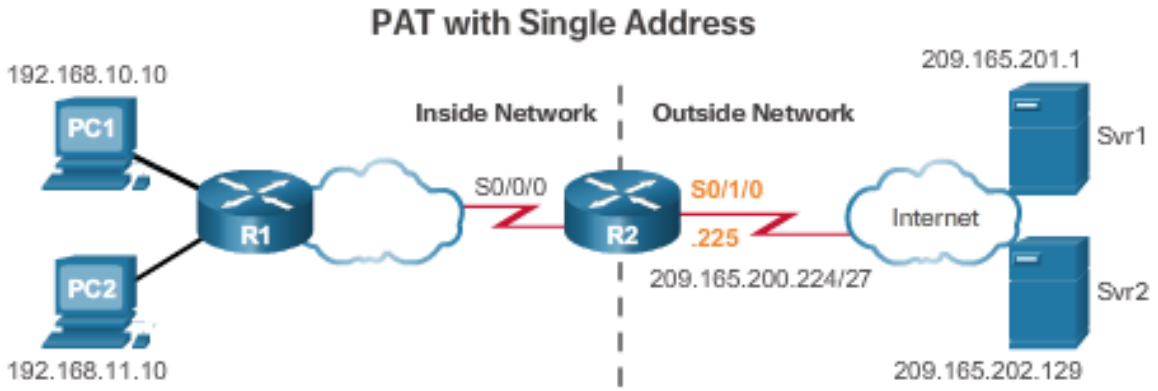
NAT – Sample Configuration

access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
[ip nat inside source list 1 s 0/1/0 overload]
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside



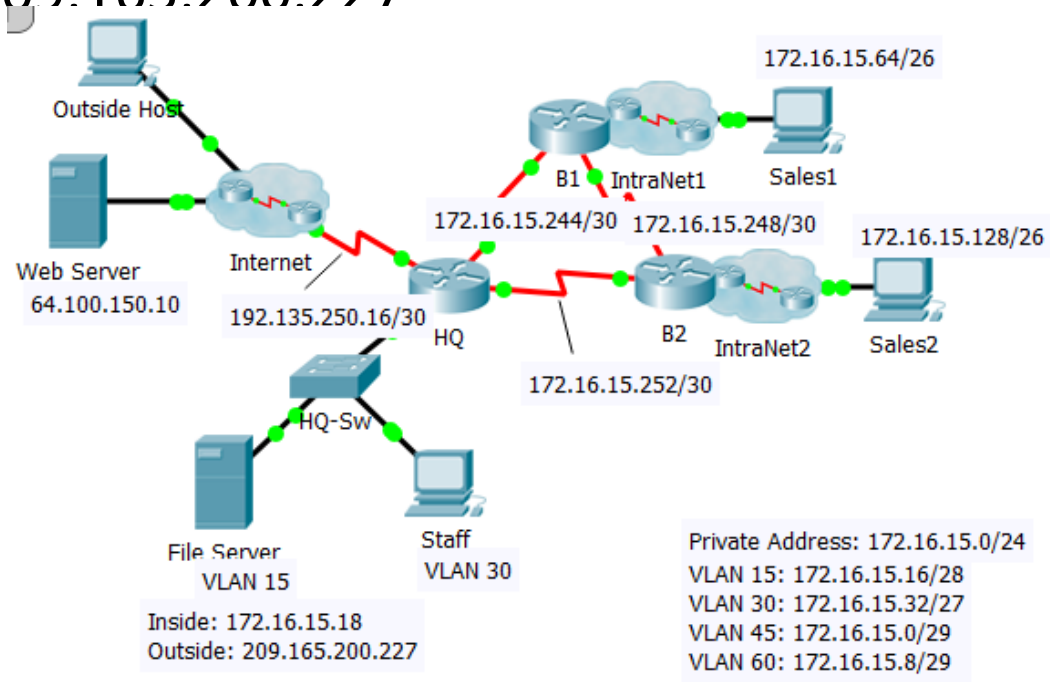
Configuring Port Address Translations (PAT) (Cont.)

- Configuring PAT: Single Address
  - Define a standard ACL to permit those addresses to be translated
    - **`access-list`** *`access-list-number`* **`permit`** *`source`* [*`source-wildcard`*]
  - Establish dynamic source translation, specify the ACL, exit interface, and overload option
    - **`ip nat inside source list`** *`access-list-number`* **`interface type`** *`name`* **`overload`**
  - Identify the inside and outside interfaces
    - **`ip nat inside`**
    - **`ip nat outside`**



NAT – Sample Configuration

access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
[ip nat inside source list 1 s 0/1/0 overload]
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside



Summary

This chapter described:

- Basic Routing
- Open Shortest Path First (OSPF)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)