TNE20003 - Internet and Cybersecurity for Engineering Applications

DHCP (Dynamic Host Configuration Protocol)

&

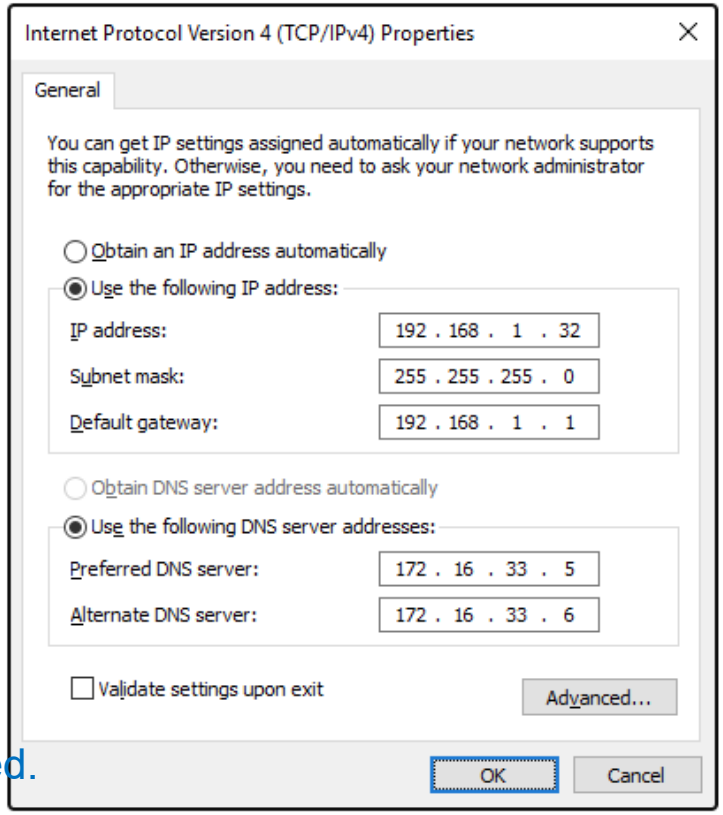
NAT (Network Address Translation)

Static and Dynamic Addressing

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Static and Dynamic Addressing

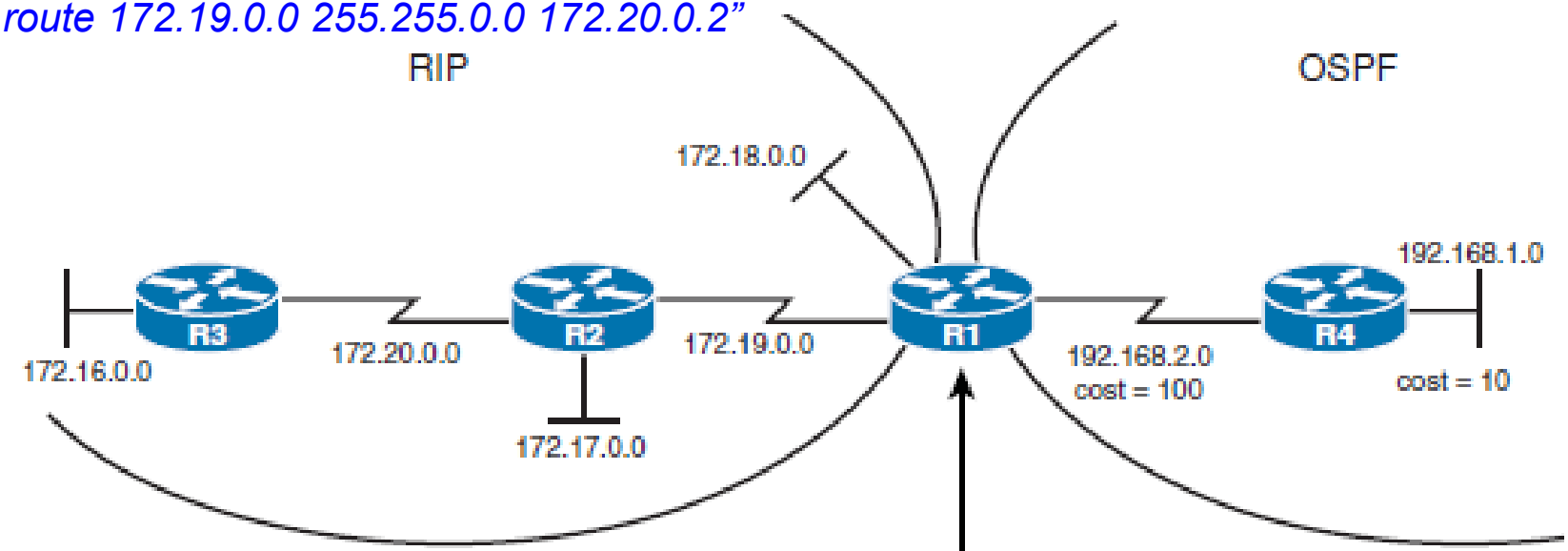
- IPv4 addresses can be assigned either statically or dynamically.
- With a static assignment, the host IPv4 address must be configured manually, together with subnet mask, default gateway, and DNS server address.
- Static addresses are typically assigned for printers, servers, and other networking devices that need to retain a fixed IP address to provide services.
- Static assignment can be time consuming to implement. It is prone to errors because manual configuration is required.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

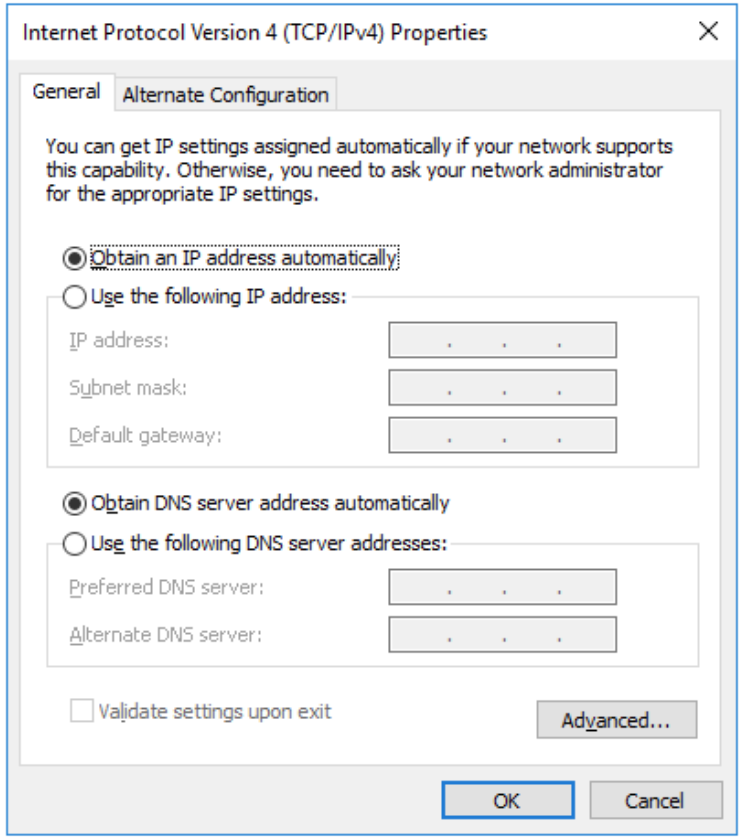
Static Addressing

- Static routes on a router.
  - Placed into the router to allow it to have paths to all of the different networks/subnets in their system.
  - Eg on R3 you would have "*ip route 192.168.1.0 255.255.255.0 172.20.0.2*"
  - & "*ip route 192.168.2.0 255.255.255.0 172.20.0.2*"
    & "*ip route 172.19.0.0 255.255.0.0 172.20.0.2*"
  - &



Dynamic Addressing

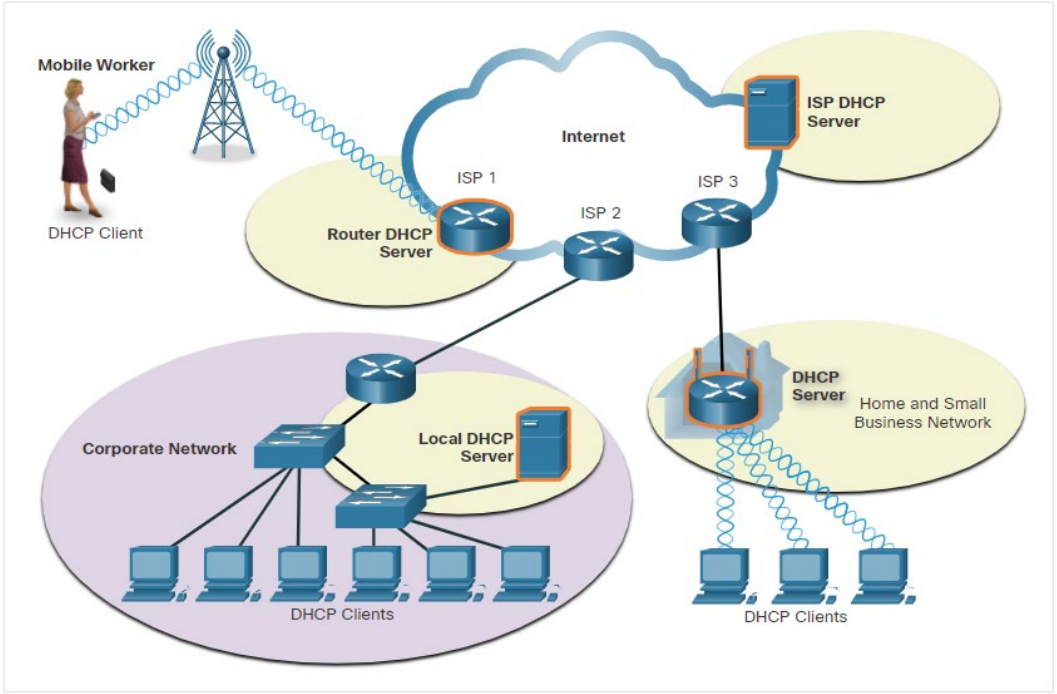
- IPv4 addresses can be dynamically assigned to end devices through an application protocol known as Dynamic Host Configuration Protocol (DHCP).
- DHCP automatically assigns addressing information such as IPv4 address, subnet mask, default gateway, and other configuration information.
- Benefits of using DHCP include:
  - Reduces the burden on network support staff and virtually eliminates entry errors.
  - A dynamic IP address is not permanently assigned to a host but is only leased for a period of time. This means when that host stops being used then the address goes back into the pool.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Dynamic Addressing

- A device can be a DHCP server if it is running the DHCP service software.
- DHCPv4 servers are typically connected to a LAN because it uses broadcast. DHCPv4 servers deployed outside of a LAN will require relay service.
- In a home network or SOHO, a wireless router provides DHCP service to end devices. It is also a DHCP client to get IPv4 address from ISP.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

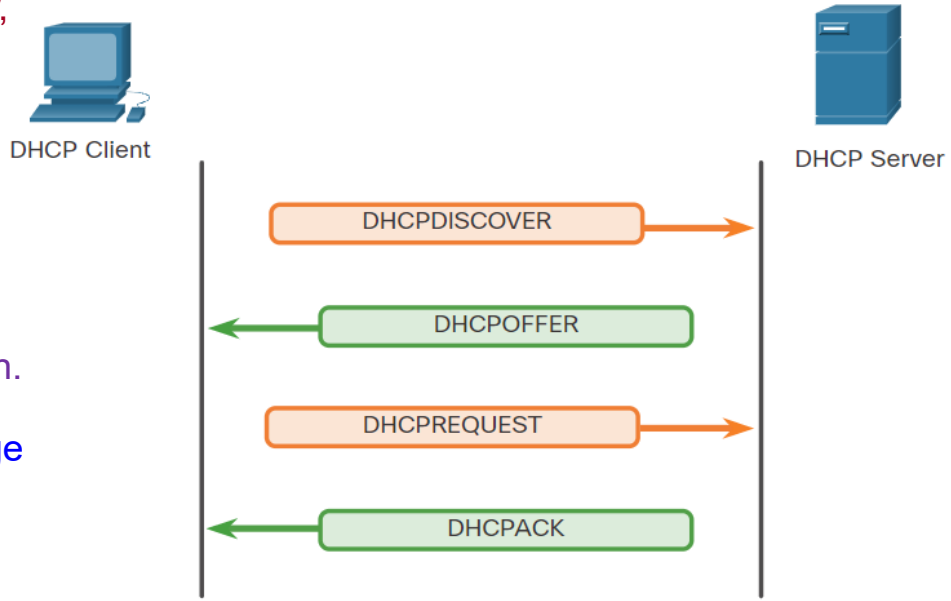
DHCPv4 Configuration

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCPv4 Configuration

When a host is configured using DHCP, it will try to obtain an IPv4 address, subnet mask, default gateway, and other options from a DHCP server. The process is as follows:

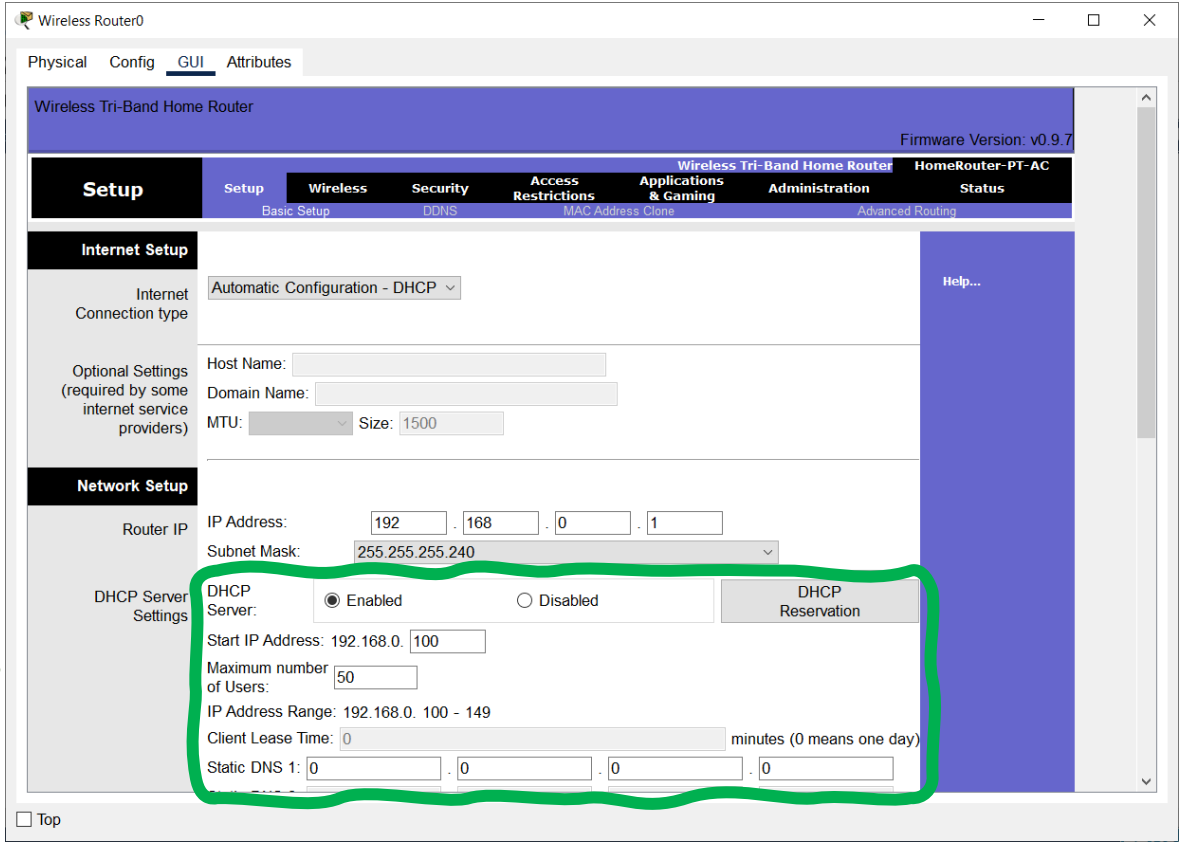
1. The client sends a **DHCPDISCOVER** message using broadcast.
2. A DHCP server responds with a **DHCPOFFER** message with a set of IPv4 addressing information.
3. The client then sends a **DHCPREQUEST** message to request the use of IPv4 addressing information offered by the DHCP server.
4. The DHCP server responds with a **DHCPACK** message to grant the request from the client.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

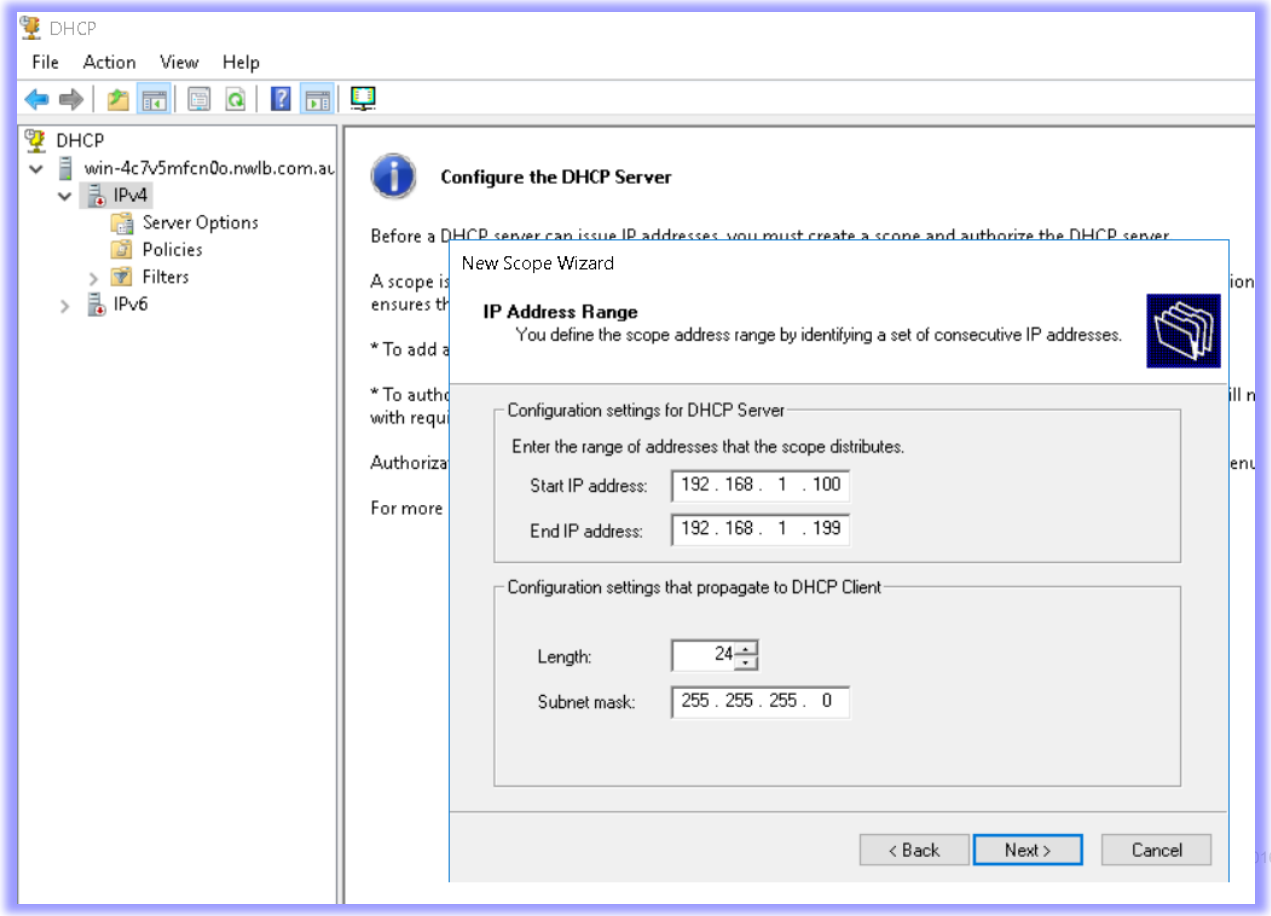
DHCPv4 Configuration - Basic *or* SOHO

- To configure a home wireless router, access its graphical web interface by opening the browser and entering the router default IPv4 address: 192.168.0.1 in the IP Address field.
- The IPv4 address of 192.168.0.1 and subnet mask of 255.255.255.0 are the defaults for the internal router interface.
  This is the default gateway for all hosts on the local network. Ensure the DHCP server is enabled.
- Specify the DHCP IPv4 address **range** with a **starting address** and the **number** of addresses to be assigned. *(do not use 192.168.0.1 because the router is already assigned this address)*



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCPv4 Configuration - Intermediate, in the Enterprise.

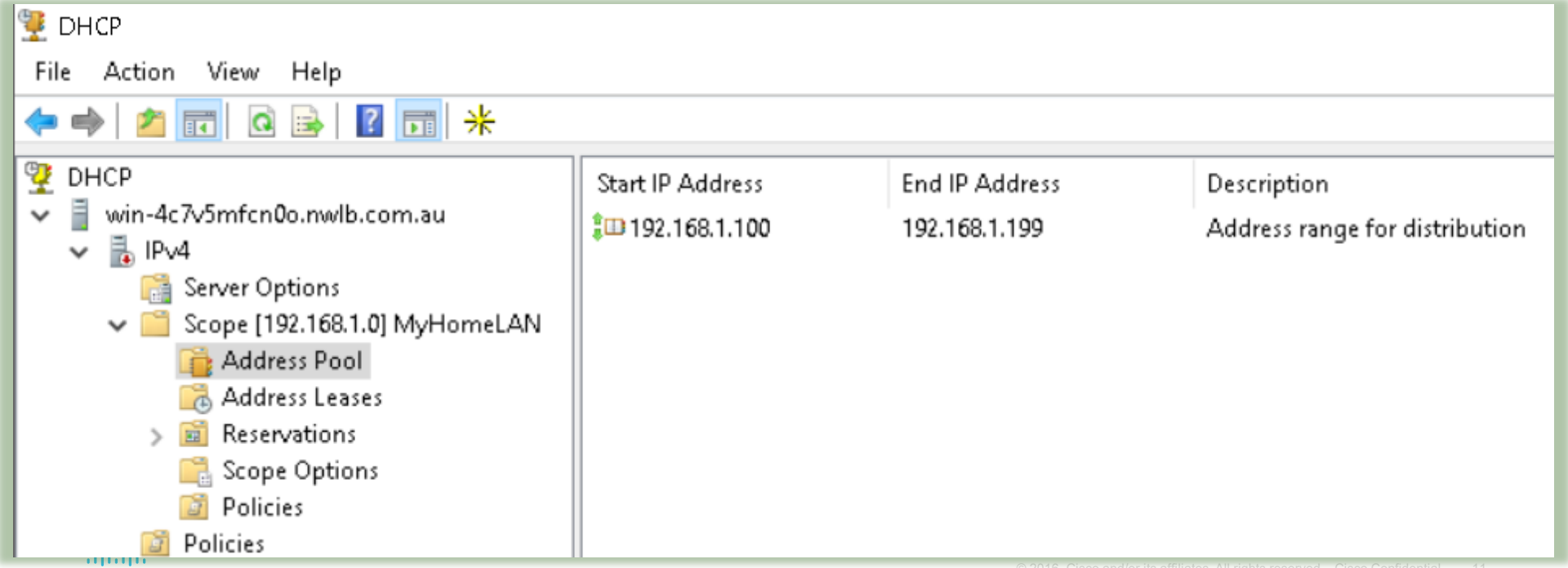


The ‘New Scope’ wizard asks all the right questions…

016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCPv4 Configuration - Intermediate, in the Enterprise.

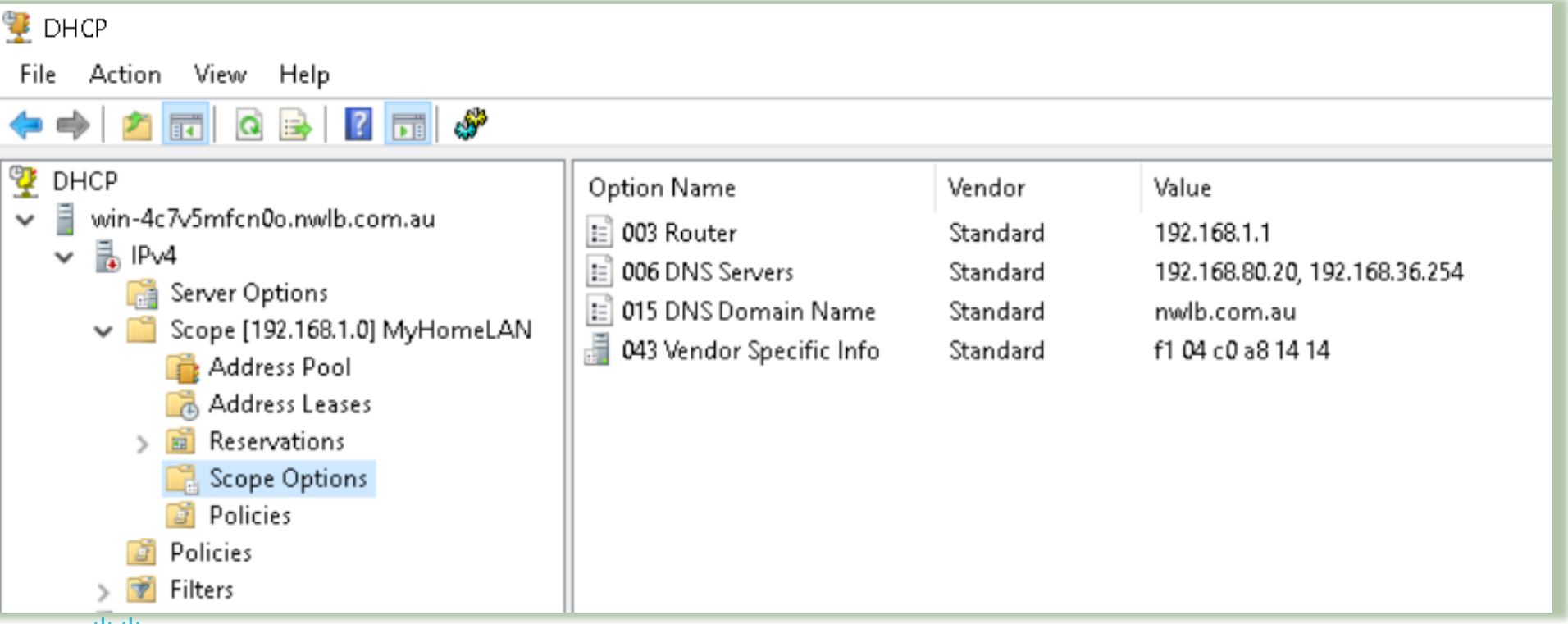
This is what it looks like during the process.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCPv4 Configuration - Intermediate, in the Enterprise.

This is what it looks like once the wizard is complete.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCPv4 Configuration - Advanced, CLI on a Router…

```
ip dhcp excluded-address 192.168.1.1 192.168.1.99
ip dhcp excluded-address 192.168.1.201 192.168.1.254
!
!
ip dhcp pool MyPool
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 200.200.200.53 153.27.201.89
 netbios-name-server 200.200.200.50
 domain-name MyCompany.com.au
 option 150 200.200.200.69
 lease 0 1
```

☝ What IP addresses **NOT** to give out - inclusive

☜ Scope or Pool name

☜ Network ID

☜ Gateway

☜ DNS servers

☜ WINS servers

☜ Standard DHCP options

☜ lease time - days hours minutes

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DHCP Summary

- IPv4 addresses can be assigned either statically or dynamically.
- A static assignment must be manually configured on a host.
- When using static IPv4 addressing, maintain an accurate list of which IPv4 addresses are assigned to which devices is difficult.
- Dynamic addressing uses DHCP to provides automatic assignment of addressing information such as IPv4 address, subnet mask, default gateway, and other IPv4 networking parameters.
- DHCP can allocate IP addresses for a configurable period of time, called a lease period.
- Many networks use both DHCP and static addressing. DHCP is used for general purpose hosts, such as end user devices. Static addressing is used for network devices, such as gateway routers, switches, servers, and printers.
- A DHCPv4 client and DHCPv4 servers use DHCP messages to initiate and complete a dynamic IPv4 addressing assignment.

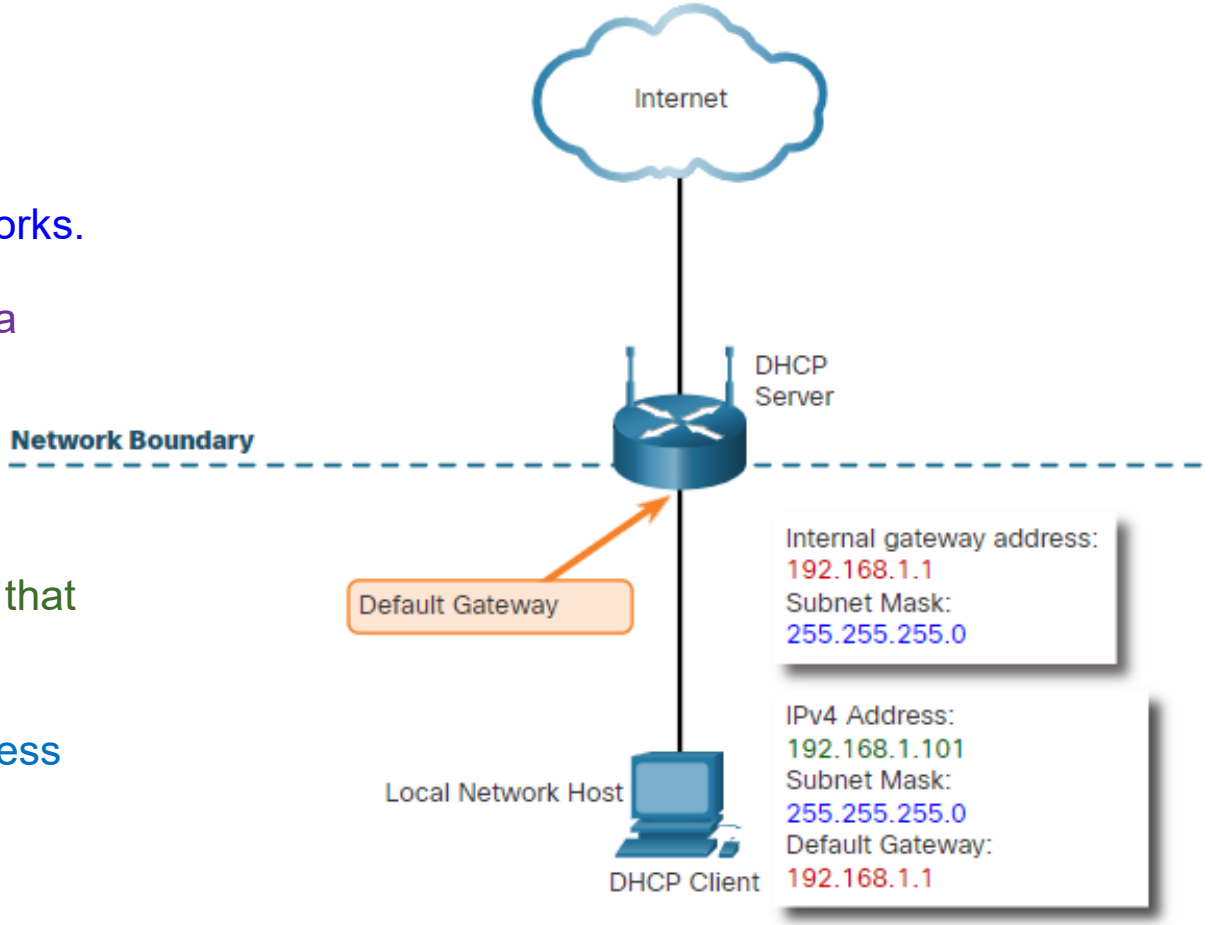
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Boundaries

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

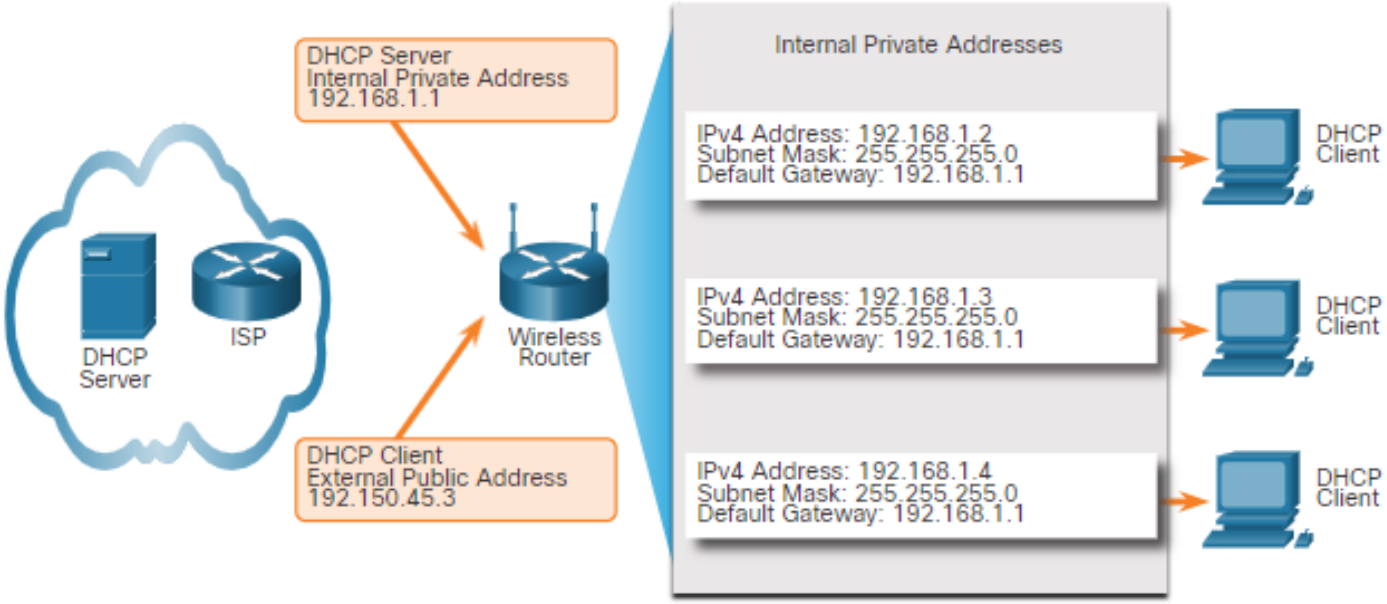
Network Boundaries

- Routers are used to connect networks.
- Each router interface connects to a separate network.
- The IPv4 address assigned to the interface is the default gateway address for all hosts connected to that same network.
- Hosts commonly get an IPv4 address using DHCP.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Boundaries



- A wireless router commonly provides IP addressing information for local internal hosts.
- A router that connects to the internet commonly gets addressing information using DHCP from the internet provider.

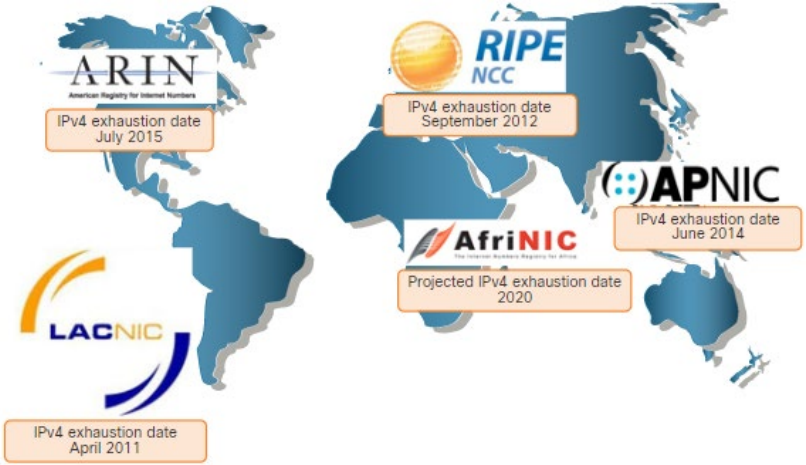
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPv4 Issues

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPv4 limitations & Temporary Solutions:

- **IPv4 address depletion** – We have basically run out of IPv4 addressing.
- **Lack of end-to-end connectivity** – To make IPv4 survive this long, private addressing and NAT were created. This ended direct communications with public addressing.
- **Increased network complexity** – Network Address Translation was meant as temporary solution and creates issues on the network as a side effect of manipulating the network headers addressing. NAT causes latency and troubleshooting issues.



© 2016 Cisco and/or its affiliates. All

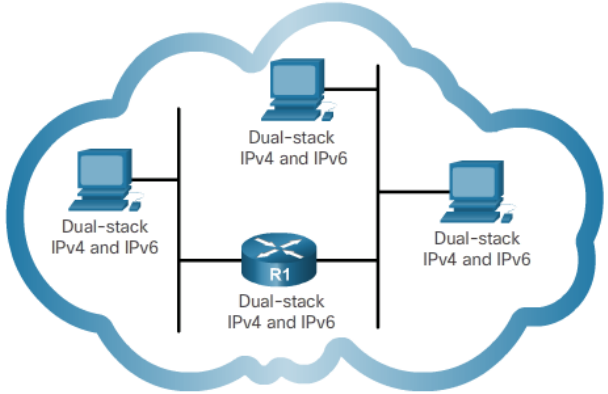
New Solution to IPv4 problem is IPv6

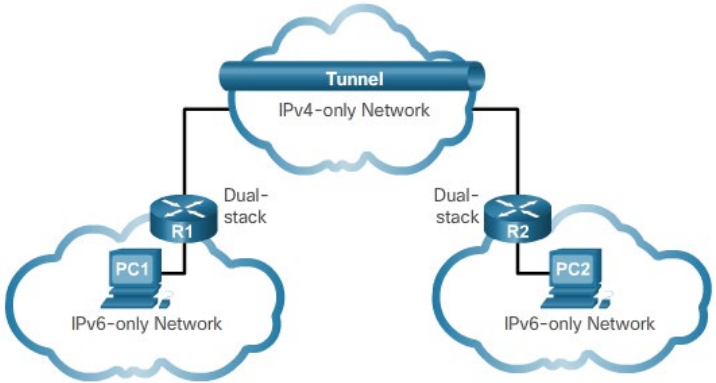
- IPv6 was developed by Internet Engineering Task Force (IETF).
- IPv6 overcomes the limitations of IPv4.
  - 4 billion IPv4 addresses
    4,000,000,000
  - 340 undecillion IPv6 addresses
    340,000,000,000,000,000,000,000,000,000,000,000,000
  - Current World Population - March 2021
    7,852,291,814
  - **Improvements that IPv6 provides:**
    - **Increased address space** – 128-bit address, not 32-bits
    - **Improved packet handling** – simplified header with fewer fields
    - **Eliminates the need for NAT** – since there is a huge amount of addressing, there is no need to use private addressing internally and be mapped to a shared public address…

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPv4 Issues

- The Need for IPv6
  - Depletion of IPv4 address space
  - Internet of Everything
- IPv4 and IPv6 Coexistence
  - Dual Stack – IPv4 and IPv6 on the same network
  - Tunneling – IPv6 packets inside IPv4 packets
  - Translation - IPv6 packet is translated to an IPv4 packet, and vice versa.





© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Address Translation - explained

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPv4 Private Address Space

A number of companies found that most of their communications was internal so no need to buy real external IP addresses.

Hence the central bodies decided to provide Private address spaces for internal use ONLY and NOT to be advertised on the real internet.

Private Internet addresses are defined in RFC 1918:

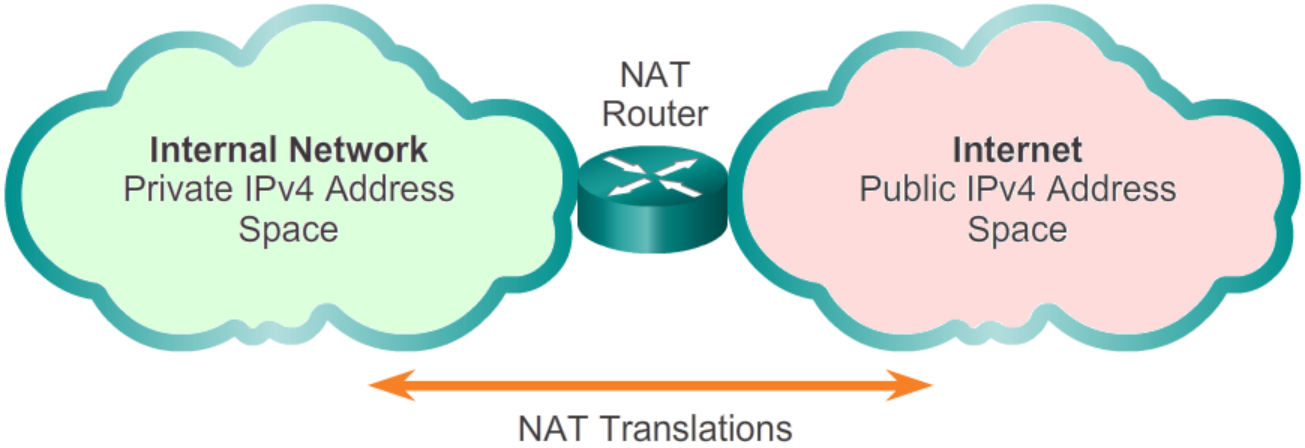
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

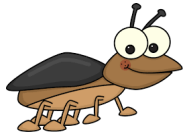
IPv4 Private Address Space

As networking evolved so too did the need to communicate from these private address spaces to the outside world. This meant there was a need for more IPv4 addresses which were now scarce.

Hence the need for Network Address Translation (NAT)



What is NAT?



- NAT is a process used to translate network addresses.
- NAT's primary use is to conserve public IPv4 addresses.
- NAT is usually implemented at border network devices, such as firewalls or routers.
- NAT allows the networks to use private addresses internally, only translating to public addresses when needed.
- Devices within the organization can be assigned private addresses and operate with locally unique addresses.
- When traffic must be sent or received to or from other organizations or the Internet, the border router translates the addresses to a public and globally unique address.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

NAT Terminology

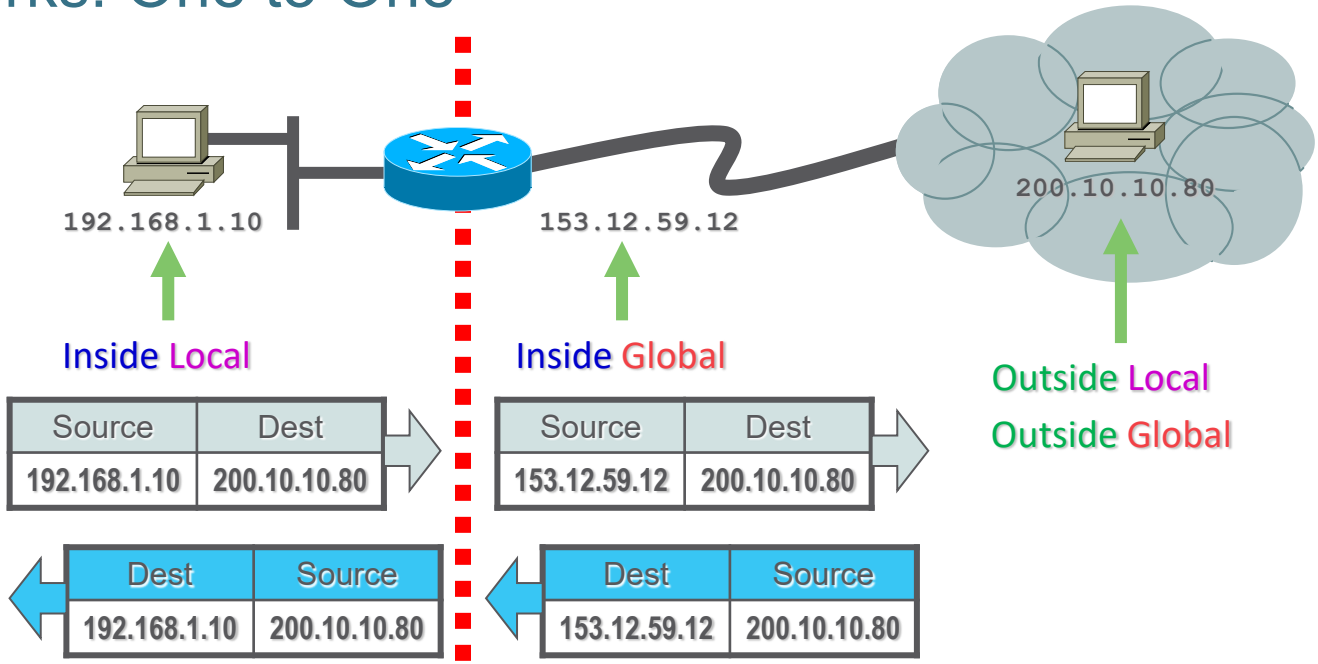
- **Inside Local Address** – The IP address assigned to a host on the inside network. Usually not an IP address assigned by the (NIC) or service provider. This address are typically private address.
- **Inside Global Address** – A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.
- **Outside Local Address** – The IP address of an outside host as it known to the hosts in the inside network.
- **Outside Global Address** – The IP address assigned to a host on the outside network. The owner of the host assigns this address.

Inside or Outside of your Administration control !

NOT **your inside or outside interfaces !!!**

rights reserved. Cisco Confidential

How it Works: One to One




```
Router# show ip nat translations
Pro Inside Global    Inside Local     Outside Local    Outside Global
--- 153.12.59.12     192.168.1.10     200.10.10.80     200.10.10.80
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Major NAT and PAT Features.

Network Address Translation

- NAT translations can be either Dynamic or Static.
- Static NAT is designed to allow one-to-one mapping of local and global addresses.
- Useful for hosts which must have a consistent address that is accessible from the Internet. Such hosts may be enterprise servers or networking devices.
- Dynamic NAT is designed to map a private IP address to a public address. Any IP address from a pool of public IP addresses is assigned to a network host.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

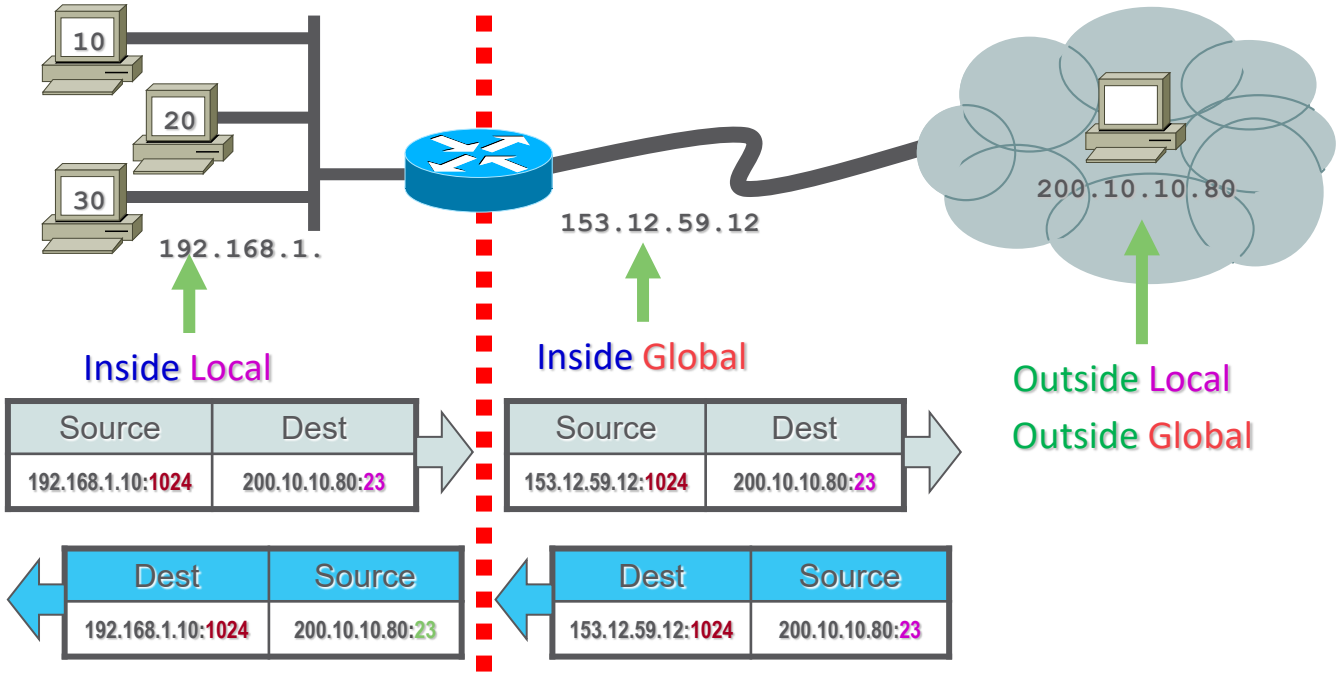
Major NAT and PAT Features…

Port Address Translation

- Overloading, or Port Address Translation (PAT), maps multiple private IP addresses to a Single public IP address.
- The multiple addresses can be mapped to a single address because each private address is tracked by its port number.
- The port number is encoded in 16 bits (65,535 ports per IP address). Practically, ports per single IP address is 4,095.
- PAT will attempt to preserve the original source port. If the source port is in use, the first available port is assigned.
- When there are no more ports available, PAT moves to the next IP address to try to allocate the original source port again, until all IPs are saturated (4095 x Total IPs in pool).

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

How it Works: Many to One




```
Router# show ip nat translations
Pro   Inside Global       Inside Local        Outside Local      Outside Global
tcp   153.12.59.12:1024   192.168.1.10:1024   200.10.10.80:23    200.10.10.80:23
tcp   153.12.59.12:1025   192.168.1.20:1024   200.10.10.80:23    200.10.10.80:23
udp   153.12.59.12:1026   192.168.1.30:1024   200.10.10.80:53    200.10.10.80:53
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

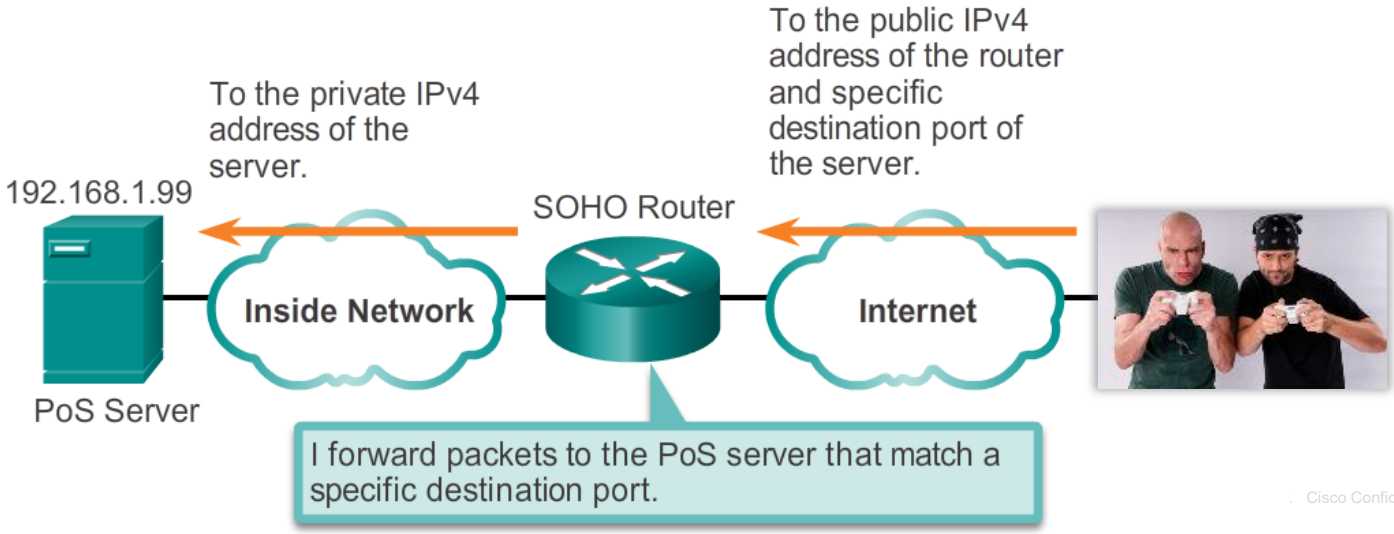
Major NAT and PAT Benefits.

- Eliminates re-assigning each host a new IP address when changing to a new ISP.
- NAT eliminates the need to re-address all hosts that require external access, saving time and money.
- Conserves addresses through application port-level multiplexing.
  With PAT, internal hosts can share a single public IP address for all external communications.
- Protects network security. Because private networks do not advertise their addresses or internal topology.

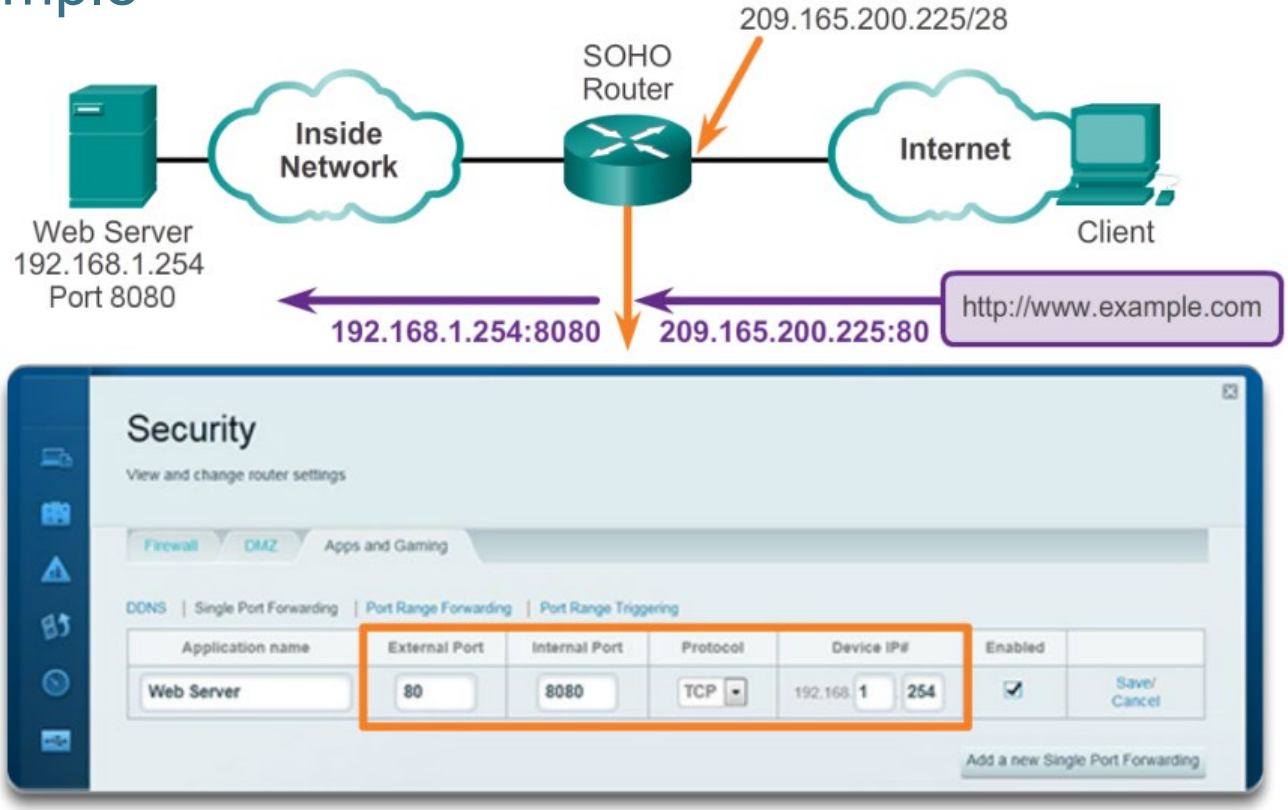
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Port Forwarding

- Port forwarding is the act of forwarding a network port from one network node to another.
- A packet sent to the public IP address and port of a router can be forwarded to a private IP address and port in inside network.
- Port forwarding is helpful in situations where servers have private addresses, not reachable from the outside networks.



SOHO Example



...and for Cisco IOS:-

```
ip nat inside source static tcp 192.168.1.254 8080 209.165.200.225 80
ip nat inside source static tcp 192.168.1.254 8080 interface Fa0/0 80
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IPv4 and NAT/PAT

- Routers create network boundaries.
- The IP address on a router interface that connects to an internal (inside) network is the default gateway address for all hosts on that same network.
- The IP address assigned to the internet side of a router such as a wireless router is the external, or outside, network.
- Network Address Translation (NAT) is used co convert private IP addresses used on an internal network to a public (global) address that can be routed through the internet.
- With PAT one single public address can be used for many internal hosts.
- Public IPv4 addresses have been scarce for some time.
- An IPv6 address is 128 bits and does not require NAT.
- Dual stack allows IPv4 and IPv6 networks to coexist.
- Tunneling is a method used to transport an IPv6 packet over an IPv4 network.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential