Chapter 15: IP Services

Instructor Materials

CCNP Enterprise: Core Networking

Chapter 15 Content

This chapter covers the following content:

Time Synchronization - This section describes the need for synchronizing time in an environment and covers Network Time Protocol and its operations to keep time consistent across devices.

First-Hop Redundancy Protocol - This section gives details on how multiple routers can provide resilient gateway functionality to hosts at the Layer 2/Layer 3 boundaries.

Network Address Translation (NAT) - This section explains how a router can translate IP addresses from one network realm to another.

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

Time Synchronization

- A device's system time is used to measure periods of idle state or computation. It is important that time is consistent on a system because applications often use the system time to tune internal processes.
- The rate a device can maintain its time can deviate from device to device. Time intervals can vary from one device to another and the times would eventually begin to drift away from each other.

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

Time Synchronization

It is important that a device's system time is consistent, and from the perspective of managing a network, that the time be synchronized between network devices for the several reasons:

- Managing passwords that change at specific time intervals
- Encryption key exchanges
- Checking validity of certificates based on expiration date and time
- Correlation of security-based events across multiple devices (routers, switches, firewalls, network access control systems, and so on)
- Troubleshooting network devices and correlating events to identify the root cause of an event

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

Network Time Protocol and Stratums

- Network Time Protocol (NTP) is used to synchronize a set of network clocks in a distributed client/server architecture.
- NTP is a UDP-based protocol that connects with servers on port 123. The client source port is dynamic.
- NTP is based on a hierarchical concept of communication. At the top of the hierarchy are authoritative devices that operate as an NTP server with an atomic clock. The NTP client queries the NTP server for its time and then updates its time based on the response.
- The NTP synchronization process is not fast, gaining an accuracy of tens of milliseconds requires hours or days of comparisons.
- Stratums are used to identify the accuracy of the time clock source. NTP servers directly attached to an authoritative time source are stratum 1 servers.
- An NTP client that queries a stratum 1 server is considered a stratum 2 client.
- The higher the stratum, the greater the chance of deviation in time from the authoritative time source due to the number of time drifts between the NTP stratums.

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

NTP Configuration

To configure an NTP client use the global command **ntp** *ip-address* [**prefer**] [**source** *interface-id*]. The keywork **prefer** indicates which NTP server to use for time synchronization. The command **ntp master** *stratum-number* to statically set the stratum for a device when it acts as an NTP server.

Example 15-1 *Simple Multi-Stratum NTP Configuration*

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ntp master 1
```

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# ntp server 192.168.1.1
```

```
R3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# ntp server 192.168.2.2 source loopback 0
```

```
R4# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)# ntp server 192.168.1.1
```

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

NTP Status and Associations

The command **show ntp status** displays the status of the NTP service. It shows the following:

- Whether the hardware clock is synchronized to the software clock, the stratum reference of the local device, and the reference clock identifier (local or IP address)
- The frequency and precision of the clock
- The NTP uptime and granularity
- The reference time
- The clock offset and delay between the client and the lower-level stratum server
- Root dispersion and peer dispersion
- NTP loopfilter
- Polling interval and time since last update

Example 15-2 *Viewing NTP Status*

```
R1# show ntp status
Clock is synchronized, stratum 1, reference is .LOCL.
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 2893800 (1/100 of seconds), resolution is 4000
reference time is E0E2D211.E353FA40 (07:48:17.888 EST Wed Jul 24 2019)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.24 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 4 sec ago.
```

```
R2# show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.1
nominal freq is 250.0000 Hz, actual freq is 249.8750 Hz, precision is 2**10
ntp uptime is 2890200 (1/100 of seconds), resolution is 4016
reference time is E0E2CD87.28B45C3E (07:28:55.159 EST Wed Jul 24 2019)
clock offset is 1192351.4980 msec, root delay is 1.00 msec
root dispersion is 1200293.33 msec, peer dispersion is 7938.47 msec
loopfilter state is 'SPIK' (Spike), drift is 0.000499999 s/s
system poll interval is 64, last update was 1 sec ago.
```

```
R3# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.2.2
nominal freq is 250.0000 Hz, actual freq is 250.0030 Hz, precision is 2**10
ntp uptime is 28974300 (1/100 of seconds), resolution is 4000
reference time is E0E2CED8.E147B080 (07:34:32.880 EST Wed Jul 24 2019)
clock offset is 0.5000 msec, root delay is 2.90 msec
root dispersion is 4384.26 msec, peer dispersion is 3939.33 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000012120 s/s
system poll interval is 64, last update was 36 sec ago.
```

A streamlined version of the NTP server status and delay can be viewed using the command **show ntp associations**.

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

Stratum Preference

An NTP client configured with multiple NTP servers will only use the NTP server with the lowest stratum.

If R2 crashes, preventing R4 from reaching R1, R4 will synchronize with R3 and become a stratum 4 time device. When R2 recovers, R4 will synchronize with R1 and become a stratum 2 device again.

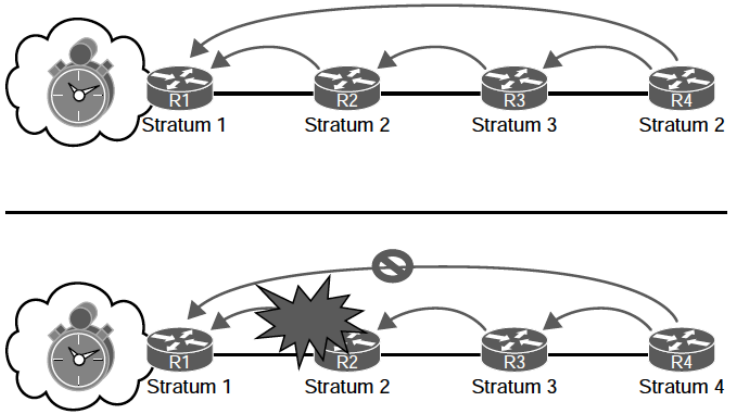

Figure 15-2 *NTP Stratum Preferences*

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

NTP Peers

An NTP client will change it's time to that of the NTP server. However, an NTP server does not change its time to reflect an NTP client. NTP peers act as clients and servers to each other. They can query and synchronize their time to each other. NTP peers are configured with the command **ntp peer** *ip-address*.

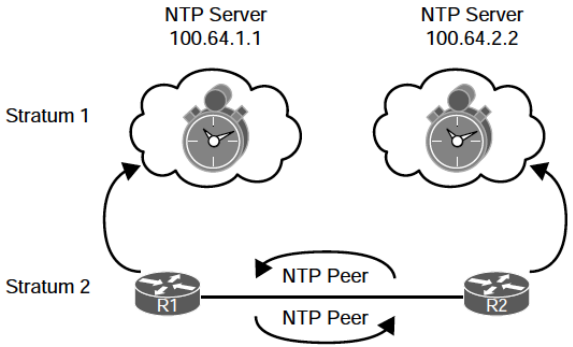

Figure 15-3 *NTP Stratums*

Example 15-4 *NTP Peer Configuration*

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ntp peer 192.168.2.2
```

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# ntp peer 192.168.1.1
```

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

First-Hop Redundancy Protocol

- Network resiliency is a key component of network design.
- Network resiliency can be accomplished by adding redundant devices such as Layer 2 switches or Layer 3 routers into a topology.

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

Network Resiliency/First Hop Redundancy Protocols

The figure shows the concept of adding resiliency to the network. In both scenarios:

- Two devices (172.16.1.2 and 172.16.1.3) can be the PC's gateway.
- There are two resilient Layer 2 links that connect SW6 to a switch that can connect the PC to either gateway.

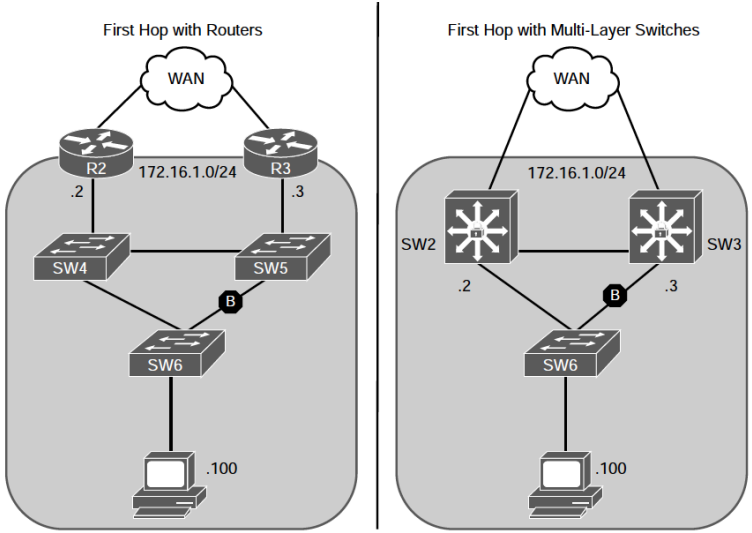

Figure 15-4 *Resiliency with Redundancy with Layer 2 and Layer 3 Devices*

First-hop redundancy protocols (FHRPs) solve the problem of end devices configuring multiple gateways. They do this by creating a virtual IP (VIP) gateway that is shared between the Layer 3 devices. The following are FHRPs:

- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Gateway Load Balancing Protocol (GLBP)

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

Object Tracking

Object tracking offers a flexible and customizable mechanism for linking with FHRPs and other routing components.

Users can track specific objects in the network and take necessary action when any object's state change affects the network traffic.

To track routes in the routing table use the command **track** *object-number* **ip route** *route/prefix-length* **reachability**. The status of object tracking can be viewed with the command **show track** [*object-number*].

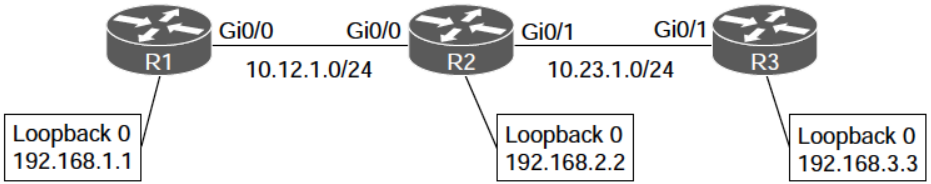

Figure 15-5 *Object Tracking*

Example 15-5 *Tracking R3's Loopback Interface*

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# track 1 ip route 192.168.3.3/32 reachability
```

```
R1# show track
Track 1
  IP route 192.168.3.3 255.255.255.255 reachability
  Reachability is Up (EIGRP)
    1 change, last change 00:00:32
  First-hop interface is GigabitEthernGi0/0
```

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

Tracking an Interface

To track an interface's line protocol state use the command **track** *object-number* **interface** *interface-id* **line-protocol**.

The example shows R2 being configured for tracking the Gi0/1 interface toward R3.

Shutting down R2's Gi0/1 interface changed the tracked object state on R1 and R2 to a down state.

Object tracking works with protocols such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP). They take action when the state of an object changes.

Example 15-6 *Tracking R2's Gi0/1 Interface Line Protocol State*

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# track 2 interface GigabitEthernGi0/1 line-protocol
```

```
R2# show track
Track 2
  Interface GigabitEthernGi0/1 line-protocol
  Line protocol is Up
    1 change, last change 00:00:37
```

Example 15-7 *Demonstrating a Change of Tracked State*

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface GigabitEthernGi0/1
R2(config-if)# shutdown
*03:04:18.975: %TRACK-6-STATE: 2 interface Gi0/1 line-protocol Up -> Down
*03:04:18.980: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.23.1.3
(GigabitEthernGi0/1) is * 03:04:20.976: %LINK-5-CHANGED: Interface
GigabitEthernGi0/1, changed state to administratively down
* 03:04:21.980: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernGi0/1,
changed state to down
```

```
R1#
03:04:24.007: %TRACK-6-STATE: 1 ip route 192.168.3.3/32 reachability Up -> Down
```

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

Hot Standby Router Protocol

Hot Standby Routing Protocol (HSRP) is a Cisco proprietary protocol. It provides routing redundancy for hosts configured with a default gateway IP address.

- A minimum of two devices are required to enable HSRP:
  - One device acts as the active device and takes care of forwarding the packets.
  - The other acts as a standby that is ready to take over the role of active device in the event of a failure.
- A virtual IP address is configured on each HSRP-enabled interface that belongs to the same HSRP group. A virtual MAC address is also assigned for the group.
- The active router receives and routes the packets destined for the virtual MAC address of the group.
- HSRP-enabled interfaces send and receive multicast UDP-based hello messages to detect any failure and designate active and standby routers.
- When the HSRP active router fails, the HSRP standby router assumes control of the virtual IP address and virtual MAC address of the group.

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

HSRP Elections & Versions

- A HSRP election selects the router with the highest priority (default is 100).
- In the event of a tie in priority, the router with the highest IP address for the network segment is preferred.
- HSRP does not support preemption by default. If a router with a lower priority becomes active, it stays active regardless if the superior router comes back online.
- The transition of the HSRP active to the standby is transparent to all hosts on the segment because the MAC address moves with the virtual IP address.
- HSRP has two versions, HSRPv1 and HSRPv2.

Table 15-2 HSRP Versions

	HSRPv1	HSRPv2
Timers	Does not support millisecond timer values	Supports millisecond timer values
Group range	0 to 255	0 to 4095
Multicast address	224.0.0.2	224.0.0.102
MAC address range	0000.0C07.AC*xy*, where *xy* is a hex value representing the HSRP group number	0000.0C9F.F000 to 0000.0C9F.FFFF

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

Configuring HSRP Virtual IP Address

The following steps show how to configure an HSRP virtual IP (VIP) gateway instance:

Step 1. Define the HSRP instance by using the command **standby** *instance-id* **ip** *vip-address*.

Step 2. (Optional) Configure HSRP router preemption with the command **standby** *instance-id* **preempt**.

Step 3. (Optional) Configure the HSRP priority by using the command **standby** *instance-id* **priority** *priority*. The priority is a value between 0 and 255.

Step 4. (Optional) Configure the HSRP MAC address with the command **standby** *instance-id* **mac-address** *mac-address*.

Step 5. (Optional) Define the HSRP timers by using the command **standby** *instance-id* **timers** {*seconds* | **msec** *milliseconds*}. HSRP can poll in intervals of 1 to 254 seconds or 15 to 999 milliseconds

Step 6. (Optional) Establish HSRP authentication by using the command **standby** *instance-id* **authentication** {*text-password* | **text** *text-password* | **md5** {**key-chain** *key-chain* | **key-string** *key-string*}}.

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

HSRP Configuration and State

Example 15-9 shows a basic HSRP configuration for VLAN 10 on SW1 and SW2, using the HSRP instance 10 and the VIP gateway instance 172.16.10.1.

Example 15 -10 shows the summarized HSRP status using the command **show standby** [*interface-id*] [**brief**].

The **show standby** command gives more details into the HSRP state. It includes the number of state changes, time since last state change, VIP addresses, timers, preemption, priority and group name.

Example 15-9 *Simple HSRP Configuration*

```
SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# interface vlan 10
03:55:35.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state
to down
SW2(config-if)# ip address 172.16.10.2 255.255.255.0
SW2(config-if)# standby 10 ip 172.16.10.1
03:56:00.097: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
SW2(config-if)# standby 10 preempt
```

```
SW3(config)# interface vlan 10
03:56:04.478: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state
to down
SW3(config-if)# ip address 172.16.10.3 255.255.255.0
SW3(config-if)# standby 10 ip 172.16.10.1
SW1(config-if)# standby 10 preempt
03:58:22.113: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
```

Example 15-10 *Viewing the Summarized HSRP State*

```
SW2# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100 P Standby 172.16.10.3     local           172.16.10.1
```

```
SW3# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100 P Active  local           172.16.10.2     172.16.10.1
```

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

HSRP Tracked Objects

HSRP provides the capability to link object tracking to priority.

Example 15-12 shows the configuration of SW2 where a tracked object is created against VLAN 1's interface line protocol, increasing the HSRP priority to 110, and linking HSRP to the tracked object so that the priority decrements by 20 if interface VLAN 1 goes down.

Example 15-13 shows that the HSRP group on VLAN 10 on SW2 correlates the status of the tracked object for the VLAN 1 interface.

Example 15-12 *Correlating HSRP to Tracked Objects*

```
SW2(config)# track 1 interface vlan 1 line-protocol
SW2(config-track)# interface vlan 10
SW2(config-if)# standby 10 priority 110
04:44:16.973: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
SW2(config-if)# standby 10 track 1 decrement 20
```

Example 15-13 *Verifying the Linkage of HSRP to Tracked Objects*

```
SW2# show standby
! Output omitted for brevity
Vlan10 - Group 10
  State is Active
    10 state changes, last state change 00:06:12
  Virtual IP address is 172.16.10.1
..
  Preemption enabled
  Active router is local
  Standby router is 172.16.10.3, priority 100 (expires in 9.856 sec)
  Priority 110 (configured 110)
    Track object 1 state Up decrement 20
```

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

Verifying HSRP State With Tracked Objects

Example 15-14 verifies the anticipated behavior by shutting down the VLAN 1 interface on SW2. The syslog messages indicate that the object track state changed immediately after the interface was shut down, and shortly thereafter, the HSRP role changed to a standby state.

Example 15-14 *Verifying the Change of HSRP State with Object Tracking*

```
SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# interface vlan 1
SW2(config-if)# shut
 04:53:16.490: %TRACK-6-STATE: 1 interface Vl1 line-protocol Up -> Down
 04:53:17.077: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
 04:53:18.486: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively
down
 04:53:19.488: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to down
 04:53:28.267: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
```

```
SW2# show standby
! Output omitted for brevity
Vlan10 - Group 10
  State is Standby
    12 state changes, last state change 00:00:39
..
  Active router is 172.16.10.3, priority 100 (expires in 9.488 sec)
  Standby router is local
  Priority 90 (configured 110)
    Track object 1 state Down decrement 20
  Group name is "hsrp-Vl10-10" (default)
```

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

Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) is an industry standard protocol that operates similarly to HSRP. However, the differences are as follows:

- The preferred active router controlling the VIP gateway is called the master router. All other VRRP routers are known as backup routers.
- VRRP enables preemption by default.
- The MAC address of the VIP gateway uses the structure 0000.5e00.01xx, where xx reflects the group ID in hex.
- VRRP uses the multicast address 224.0.0.18 for communication.

There are currently two versions of VRRP:

- VRRPv2: Supports IPv4
- VRRPv3: Supports IPv4 and IPv6

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

Legacy VRRP Configuration

Early VRRP configurations supported only VRRPv2 and was non-hierarchical in its configuration. The following are steps used to configure older software versions with VRRP:

Step 1. Define the VRRP instance by using the command **vrrp** *instance-id* **ip** *vip-address*.

Step 2. (Optional) Define the VRRP priority by using the command **vrrp** *instance-id* **priority** *priority*. The priority is a value between 0 and 255.

Step 3. (Optional) Enable object tracking so that the priority is decremented when the object is false by using the command **vrrp** *instance-id* **track** *object-id* **decrement** *decrement-value*.

Step 4. (Optional) Establish VRRP authentication by using the command vrrp instance-id authentication {*text-password* | **text** *text-password* | **md5** {**key-chain** *key-chain* | **key-string** *key-string*}}

Example 15-15 *Legacy VRRP Configuration*

```
R2# configure term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface GigabitEthernet 0/0
R2(config-if)# ip address 172.16.20.2 255.255.2
R2(config-if)# vrrp 20 ip 172.16.20.1
 04:32:14.109: %VRRP-6-STATECHANGE: Gi0/0 Grp 20 state Init -> Backup
 04:32:14.113: %VRRP-6-STATECHANGE: Gi0/0 Grp 20 state Init -> Backup
 04:32:17.728: %VRRP-6-STATECHANGE: Gi0/0 Grp 20 state Backup -> Master
 04:32:47.170: %VRRP-6-STATECHANGE: Gi0/0 Grp 20 state Master -> Backup
```

```
R3# configure term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# interface GigabitEthernGi0/0
R3(config-if)# ip add 172.16.20.3 255.255.255.0
 04:32:43.550: %VRRP-6-STATECHANGE: Gi0/0 Grp 20 state Init -> Backup
 04:32:43.554: %VRRP-6-STATECHANGE: Gi0/0 Grp 20 state Init -> Backup
 04:32:47.170: %VRRP-6-STATECHANGE: Gi0/0 Grp 20 state Backup -> Master
```

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

VRRP State

The command **show vrrp** [**brief**] provides an update on the VRRP group, along with other relevant information for troubleshooting. Example 15-16 shows the brief iteration of the command and 15-17 shows the detailed state of VRRP.

Example 15-16 *Viewing the Summarized VRRP State*

```
R2# show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Gi0/0              20  100 3609       Y  Backup  172.16.20.3     172.16.20.1
```

```
R3# show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Gi0/0              20  100 3609       Y  Master  172.16.20.3     172.16.20.1
```

Example 15-17 *Viewing the Detailed VRRP State*

```
R2# show vrrp
EthernGi0/0 - Group 20
  State is Backup
  Virtual IP address is 172.16.20.1
  Virtual MAC address is 0000.5e00.0114
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 172.16.20.3, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.904 sec)
```

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

Hierarchical VRRP Configuration

The newer version of IOS XE software provides configuration of VRRP in a multi-address format that is hierarchical. The following are steps to configure hierarchical VRRP:

Step 1. Enable VRRPv3 on the router by using the command **fhrp version vrrp v3**.

Step 2. Define the VRRP instance by using the command **vrrp** *instance-id* **address-family** {**ipv4** | **ipv6**}.

Step 3. (Optional) Change VRRP to Version 2 by using the command **vrrpv2**. VRRPv2 and VRRPv3 are not compatible.

Step 4. Define the gateway VIP by using the command **address** *ip-address*.

Step 5. (Optional) Define the VRRP priority by using the command **priority** *priority*.

Step 6. (Optional) Enable object tracking so that the priority is decremented when the object is false using the command **track** *object-id* **decrement** *decrement-value*.

Example 15-18 *Configuring Hierarchical VRRP Configuration*

```
SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# fhrp version vrrp v3
SW2(config)# interface vlan 22
 19:45:37.385: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan22, changed
 state to up
SW2(config-if)# ip address 172.16.22.2 255.255.255.0
SW2(config-if)# vrrp 22 address-family ipv4
SW2(config-if-vrrp)# address 172.16.22.1
SW2(config-if-vrrp)# track 1 decrement 20
SW2(config-if-vrrp)# priority 110
SW2(config-if-vrrp)# track 1 decrement 20
 19:48:00.338: %VRRP-6-STATE: Vlan22 IPv4 group 22 state INIT -> BACKUP
 19:48:03.948: %VRRP-6-STATE: Vlan22 IPv4 group 22 state BACKUP -> MASTER
```

```
SW3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)# fhrp version vrrp v3
SW3(config)# interface vlan 22
 19:46:13.798: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan22, changed state
to up
SW3(config-if)# ip address 172.16.22.3 255.255.255.0
SW3(config-if)# vrrp 22 address-family ipv4
SW3(config-if-vrrp)# address 172.16.22.1
 19:48:08.415: %VRRP-6-STATE: Vlan22 IPv4 group 22 state INIT -> BACKUP
```

The status of the VRRP routers can be viewed with the command **show vrrp** [**brief**]. The output is identical to that of the legacy VRRP configuration.

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

Global Load Balancing Protocol

Global Load Balancing Protocol (GLBP) provides gateway redundancy and load-balancing capability to a network segment. It does this with an active/standby gateway and ensures that each member of the GLBP group forwards traffic to the appropriate gateway.

The GLBP has two roles:

- **Active virtual gateway (AVG):** The participating routers elect one AVG per GLBP group to respond to initial ARP requests for the VIP.
- **Active virtual forwarder (AVF):** The AVF routes traffic received from assigned hosts. A unique virtual MAC address is created and assigned by the AVG to the AVFs. The AVF is assigned to a host when the AVG replies to the ARP request with the assigned AVF's virtual MAC address. The AVFs are also recognized as Fwd instances on the routers.

GLBP supports four active AVFs and one AVG per GLBP group. A router can be an AVG and an AVF at the same time. In the event of a failure of the AVG, the AVG role is transferred to a standby AVG device. In the event of a failure of an AVF, another router takes over the forwarding responsibilities for that AVF, which includes the virtual MAC address for that instance.

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

GLBP Configuration

The following steps detail how to configure a GLBP:

Step 1. Define the GLBP instance by using the command **glbp** *instance-id* **ip** *vip-address*.

Step 2. (Optional) Configure GLBP preemption with the command **glbp** *instance-id* **preempt**.

Step 3. (Optional) Define the GLBP priority by using the command **glbp** *instance-id* **priority** *priority*. The priority is a value between 0 and 255.

Step 4. (Optional) Define the GLBP timers by using the command **glbp** *instance-id* **timers** {*hello-seconds* | **msec** *hello-milliseconds*} {*hold-seconds* | **msec** *hold-milliseconds*}.

Step 5. (Optional) Establish GLBP authentication by using the command **glbp** instance-id **authentication** {**text** *text-password* | **md5** {**key-chain** *key-chain* | **key-string** *key-string*}}.

Example 15-20 *Basic GLBP Configuration*

```
SW2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)# interface vlan 30
SW2(config-if)# ip address 172.16.30.2 255.255.255.0
SW2(config-if)# glbp 30 ip 172.16.30.1
  05:41:15.802: %GLBP-6-STATECHANGE: Vlan30 Grp 30 state Speak -> Active
SW2(config-if)#
  05:41:25.938: %GLBP-6-FWDSTATECHANGE: Vlan30 Grp 30 Fwd 1 state Listen -> Active
SW2(config-if)# glbp 30 preempt
```

```
SW3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)# interface vlan 30
SW3(config-if)# ip address 172.16.30.3 255.255.255.0
SW3(config-if)# glbp 30 ip 172.16.30.1
 05:41:32.239: %GLBP-6-FWDSTATECHANGE: Vlan30 Grp 30 Fwd 2 state Listen -> Active
SW3(config-if)# glbp 30 preempt
```

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

GLBP Status

The command **show glbp brief** shows high-level details of the GLBP group, including the interface, group, active AVG, standby AVG, and statuses of the AVFs.

The command **show glbp** displays additional information, including the timers, preemption settings, and statuses for the AVG and AVFs for the GLBP group.

Example 15-21 *Viewing the Brief GLBP Status*

```
SW2# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl30        30   -   100 Active   172.16.30.1     local           172.16.30.3
Vl30        30   1   -   Active   0007.b400.1e01  local           -
Vl30        30   2   -   Listen   0007.b400.1e02  172.16.30.3     -
```

```
SW3# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl30        30   -   100 Standby  172.16.30.1     172.16.30.2     local
Vl30        30   1   -   Listen   0007.b400.1e01  172.16.30.2     -
Vl30        30   2   -   Active   0007.b400.1e02  local           -
```

Example 15-22 *Viewing the Detailed GLBP Status*

```
SW2# show glbp
Vlan30 - Group 30
  State is Active
    1 state change, last state change 00:01:26
  Virtual IP address is 172.16.30.1
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.664 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 172.16.30.3, priority 100 (expires in 7.648 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    70b3.17a7.7b65 (172.16.30.3)
    70b3.17e3.cb65 (172.16.30.2) local
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:01:16
    MAC address is 0007.b400.1e01 (default)
    Owner ID is 70b3.17e3.cb65
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen
    MAC address is 0007.b400.1e02 (learnt)
    Owner ID is 70b3.17a7.7b65
    Redirection enabled, 597.664 sec remaining (maximum 600 sec)
    Time to live: 14397.664 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 172.16.30.3 (primary), weighting 100 (expires in 8.160 sec)
```

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

GLBP Load Balancing

GLBP supports three methods of load balancing traffic:

- **Round robin -** Uses each virtual forwarder MAC address to sequentially reply for the virtual IP address. GLBP uses round robin as the default load-balancing method.
- **Weighted -** Defines weights to each device in the GLBP group to define the ratio of load balancing between the devices. This allows for a larger weight to be assigned to bigger routers that can handle more traffic.
- **Host dependent -** Uses the host MAC address to decide to which virtual forwarder MAC to redirect the packet. This method ensures that the host uses the same virtual MAC address as long as the number of virtual forwarders does not change within the group.

The load-balancing method can be changed with the command **glbp** *instance-id* **load-balancing** {**host-dependent** | **round-robin** | **weighted**}. The weighted load-balancing method has the AVG direct traffic to the AVFs based on the percentage of weight a router has over the total weight of all GLBP routers. The weight can be set for a router with the command **glbp** *instance-id* **weighting** *weight*.

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

Verifying GLBP Weighted Load Balancing

The example shows that the load-balancing method has been changed to weighted and that the appropriate weight has been set for each AVF.

Example 15-24 *Verifying GLBP Weighted Load Balancing*

```
SW2# show glbp
Vlan30 - Group 30
  State is Active
    1 state change, last state change 00:04:55
  Virtual IP address is 172.16.30.1
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.160 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 172.16.30.3, priority 100 (expires in 9.216 sec)
  Priority 100 (default)
  Weighting 20 (configured 20), thresholds: lower 1, upper 20
  Load balancing: weighted
  Group members:
    70b3.17a7.7b65 (172.16.30.3)
    70b3.17e3.cb65 (172.16.30.2) local
There are 2 forwarders (1 active)
 Forwarder 1
   State is Active
     1 state change, last state change 00:04:44
   MAC address is 0007.b400.1e01 (default)
   Owner ID is 70b3.17e3.cb65
   Redirection enabled
   Preemption enabled, min delay 30 sec
   Active is local, weighting 20
 Forwarder 2
   State is Listen
   MAC address is 0007.b400.1e02 (learnt)
   Owner ID is 70b3.17a7.7b65
   Redirection enabled, 599.232 sec remaining (maximum 600 sec)
   Time to live: 14399.232 sec (maximum 14400 sec)
   Preemption enabled, min delay 30 sec
   Active is 172.16.30.3 (primary), weighting 80 (expires in 9.408 sec)
```

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

Network Address Translation

- In the early stages of the internet, large network blocks were assigned to organizations.
- Network engineers started to realize that as more people connected to the internet, the IP address space would become exhausted.

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

Private Network Addressing

RFC 1918 established common network blocks that are non-globally routed networks. These address blocks provide large private network blocks for companies to connect their devices together, but private IP addressing doesn't exist on the internet. The private address blocks are as follows:

10.0.0.0/8 accommodates 16,777,216 hosts.

172.16.0.0/24 accommodates 1,048,576 hosts.

192.168.0.0/16 accommodates 65,536 hosts.

NAT enables the internal IP network to appear as a publicly routed external network. A NAT device (typically a router or firewall) modifies the source or destination IP addresses in a packet's header as the packet is received on the outside or inside interface. NAT can be used in use cases other than just providing internet connectivity to private networks such as providing connectivity when a company buys another company, and the two companies have overlapping networks.

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

Network Address Translation

NAT enables the internal IP network to appear as a publicly routed external network.

A NAT device (typically a router or firewall) modifies the source or destination IP addresses in a packet's header as the packet is received on the outside or inside interface.

NAT can be used in use cases other than just providing internet connectivity to private networks, such as providing connectivity when a company buys another company, and the two companies have overlapping networks.

Most routers and switches perform NAT translation only with the IP header addressing and do not translate IP addresses within the payload (for example, DNS requests). Some firewalls can perform NAT within the payload for certain types of traffic.

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

Inside/Outside Local and Global

Here are four important terms related to NAT:

- Inside local - The actual private IP address assigned to a device on the inside network(s).
- Inside global - The public IP address that represents one or more inside local IP addresses to the outside.
- Outside local - The IP address of an outside host as it appears to the inside network. The IP address does not have to be reachable by the outside but is considered private and must be reachable by the inside network.
- Outside global - The public IP address assigned to a host on the outside network. This IP address must be reachable by the outside network.

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

Types of NAT

Three types of NAT commonly used today are as follows:

- Static NAT - Provides a static one-to-one mapping of a local IP address to a global IP address.
- Pooled NAT - Provides a dynamic one-to-one mapping of a local IP address to a global IP address. The global IP address is temporarily assigned to a local IP address. After a certain amount of idle NAT time, the global IP address is returned to the pool.
- Port Address Translation (PAT) - Provides a dynamic many-to-one mapping of many local IP addresses to one global IP address. The NAT device translates the private IP address and port to a different global IP address and port. The port is unique from any other ports, which enables the NAT device to track the global IP address to local IP addresses based on the unique port mapping.

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

NAT Example

Figure 15-7 is used throughout this section to illustrate NAT.

R5 performs the translation; its Gi0/0 interface (10.45.1.5) is the outside interface, and its Gi0/1 (10.56.1.5) interface is the inside interface. The other devices act as either clients or servers to demonstrate how NAT functions.

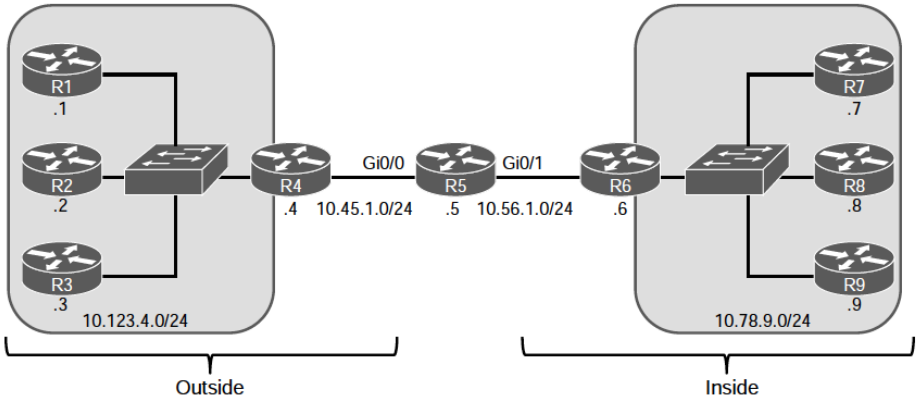

Figure 15-7 *NAT Topology*

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

NAT Example (Cont.)

Example 15-25 shows the routing tables of R1, R5 and R7.

- R1, R2, and R3 all have a static default route toward R4.
- R4 has a static default route to R5.
- R7, R8, and R9 all have a static default route to R6
- R6 has a static default route to R5.
- R5 has two static routes. One to the 10.123.4.0/24 network via R4 and the other to the 10.78.9.0/24 network via R6.

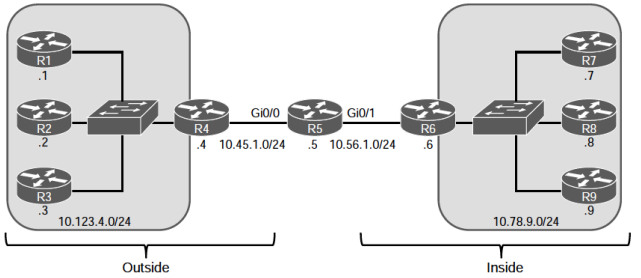

Figure 15-7 *NAT Topology*

Example 15-25 *Routing Tables of R1, R5, and R7*

```
R1# show ip route | begin Gateway
Gateway of last resort is 10.123.4.4 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.123.4.4
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.123.4.0/24 is directly connected, GigabitEthernGi0/0
```

```
R5# show ip route | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.45.1.0/24 is directly connected, GigabitEthernGi0/0
C        10.56.1.0/24 is directly connected, GigabitEthernGi0/1
S        10.78.9.0/24 [1/0] via 10.56.1.6
S        10.123.4.0/24 [1/0] via 10.45.1.4
```

```
R7# show ip route  | begin Gateway
Gateway of last resort is 10.78.9.6 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.78.9.6
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.78.9.0/24 is directly connected, GigabitEthernGi0/0
```

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

NAT Example (Cont.)

- Example 15-26 shows a traceroute from R1 to R7. The topology provides full connectivity between the outside hosts (R1, R2, and R3) and the inside hosts (R7, R8, and R9).

- Example 15-27 shows a telnet connection from R7 to R1. The local IP address reflects R1 (10.123.4.1) and the remote address is R7 (10.78.9.7) No NAT has occurred for this Telnet session.

Example 15-26 *Traceroute from R1 to R7*

```
R1# traceroute 10.78.9.7
Type escape sequence to abort.
Tracing the route to 10.78.9.7
VRF info: (vrf in name/id, vrf out name/id)
  1 10.123.4.4 1 msec 0 msec 0 msec
  2 10.45.1.5 1 msec 0 msec 0 msec
  3 10.56.1.6 1 msec 0 msec 0 msec
  4 10.78.9.7 1 msec *  1 msec
```

Example 15-27 *Viewing the Source IP Address*

```
R7# telnet 10.123.4.1
Trying 10.123.4.1 ... Open
************************************************************
* You have remotely connected to R1 on line 2
************************************************************
User Access Verification
Password:

R1# show tcp brief
TCB        Local Address               Foreign Address             (state)
F69CE570   10.123.4.1.23               10.78.9.7.49024             ESTAB
```

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

Static NAT

Static NAT involves the translation of a global IP address to a local IP address, based on a static mapping of the global IP address to the local IP address.

There are two types of static NAT:

- **Inside static NAT** - involves the mapping of an inside local (private) IP address to an inside global (public) IP address.
- **Outside static NAT** - involves the mapping of an outside global (public) IP address to an outside local (private) IP address.

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

Inside Static NAT

The steps for configuring inside static NAT are as follows:

Step 1. Configure the outside interfaces by using the command **ip nat outside**.

Step 2. Configure the inside interface with the command **ip nat inside**.

Step 3. Configure the inside static NAT by using the command **ip nat inside source static** *inside-local-ip inside-global-ip***.**

Example 15-28 *Configuring Inside Static NAT*

```
R5# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)# interface GigabitEthernGi0/0
R5(config-if)# ip nat outside
R5(config-if)# interface GigabitEthernGi0/1
R5(config-if)# ip nat inside
R5(config-if)# exit
R5(config)# ip nat inside source static 10.78.9.7 10.45.1.7
```

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

Identifying the Source with Inside Static NAT/NAT Translation Table

With NAT configured, a telnet session with R1 is initiated. Viewing the TCP session on R1, the local address remains 10.123.4.1 but the remote address now reflects 10.45.1.7.

Example 15-29 *Identification of the Source with Inside Static NAT*

```
R7# telnet 10.123.4.1
Trying 10.123.4.1 ... Open
************************************************************
* You have remotely connected to R1 on line 3
************************************************************
User Access Verification
Password:

R1# show tcp brief
TCB        Local Address               Foreign Address             (state)
F6D25D08   10.123.4.1.23               10.45.1.7.56708             ESTAB
```

The NAT translation table consists of static and dynamic entries. The NAT translation table is displayed with the command **show ip nat translations**.

- The first entry is the dynamic entry correlating to the Telnet session.
- The second entry is the inside static NAT entry that was configured.

Example 15-30 *NAT Translation Table for Inside Static NAT*

```
R5# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.45.1.7:56708    10.78.9.7:56708    10.123.4.1:23      10.123.4.1:23
--- 10.45.1.7          10.78.9.7          ---                ---
```

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

NAT Translation Steps

The NAT translation follows these steps:

Step 1. As traffic enters the Gi0/1 interface on R5, R5 performs a route lookup for the destination IP address, which points out of its Gi0/0 interface. R1 is aware that the Gi0/0 interface is an outside NAT interface and that the Gi0/1 interface is an inside NAT interface and therefore checks the NAT table for an entry.

Step 2. Only the inside static NAT entry exists, so R5 creates a dynamic inside NAT entry with the packet's destination (10.123.4.1) for the outside local and outside global address.

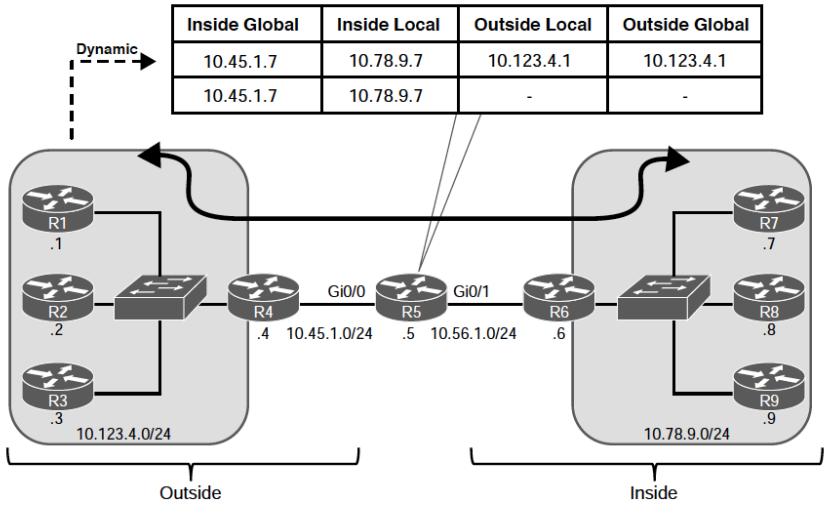

Figure 15-8 *Inside Static NAT Topology for R7 as 10.45.1.7*

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

NAT Translation Steps (Cont.)

Step 3. R5 translates (that is, changes) the packet's source IP address from 10.78.9.7 to 10.45.1.7.

Step 4. R1 registers the session as coming from 10.45.1.7 and then transmits a return packet. The packet is forwarded to R4 using the static default route, and R4 forwards the packet using the static default route.

Step 5. As the packet enters on the Gi0/0 interface of R5, R5 is aware that the Gi0/0 interface is an outside NAT interface and checks the NAT table for an entry.

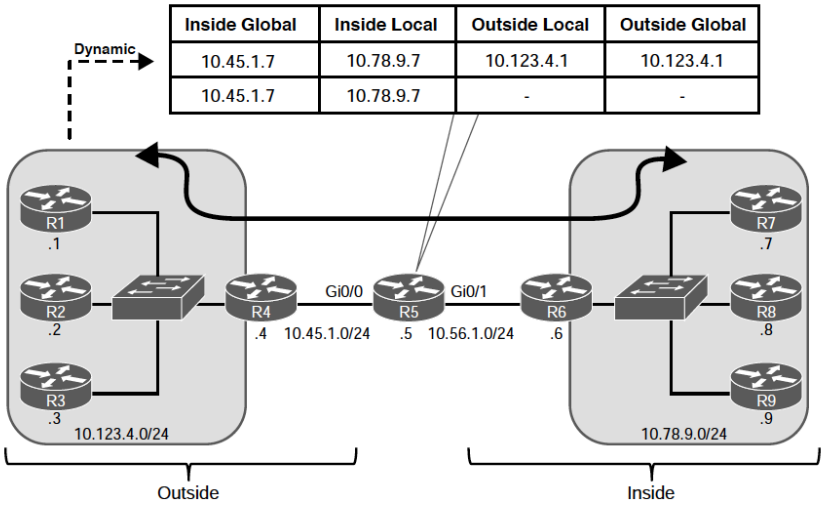

Figure 15-8 *Inside Static NAT Topology for R7 as 10.45.1.7*

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

NAT Translation Steps (Cont.)

Step 6. R5 correlates the packet's source and destination ports with the first NAT entry, as shown in Example 15-30, and knows to modify the packet's destination IP address from 10.45.1.7 to 10.78.9.7.

Step 7. R5 routes the packet out the Gi0/1 interface toward R6.

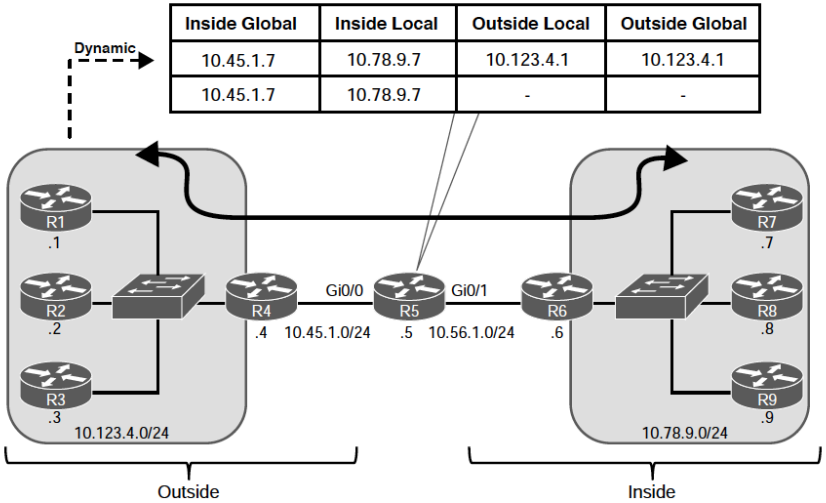

Figure 15-8 *Inside Static NAT Topology for R7 as 10.45.1.7*

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

Connectivity from External Devices to the Inside Global IP Address

In Example 15-31:

- R2 establishes a Telnet session with R7, using the inside global IP address 10.45.1.7.
- R5 simply creates a second dynamic entry for this new session.
- From R7's perspective, it has connected with R2 (10.123.4.2).

Example 15-31 *Connectivity from External Devices to the Inside Global IP Address*

```
R2# telnet 10.45.1.7
Trying 10.45.1.7 ... Open
************************************************************
* You have remotely connected to R7 on line 2
************************************************************
User Access Verification
Password:

R7# show tcp brief
TCB       Local Address               Foreign Address             (state)
F6561AE0  10.78.9.7.23                10.123.4.2.63149            ESTAB
F65613E0  10.78.9.7.33579             10.123.4.1.23               ESTAB
```

```
R5# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.45.1.7:56708    10.78.9.7:56708    10.123.4.1:23      10.123.4.1:23
tcp 10.45.1.7:23       10.78.9.7:23       10.123.4.2:63149   10.123.4.2:63149
--- 10.45.1.7          10.78.9.7          ---                ---
```

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

Outside Static NAT

Outside static NAT involves the mapping of an outside global (public) IP address to an outside local (private) IP address. The steps for configuring outside static NAT are as follows:

Step 1. Configure the outside interfaces by using the command **ip nat outside**.

Step 2. Configure the inside interface with the command **ip nat inside**.

Step 3. Configure the outside static NAT by using the command **ip nat outside source static** *outside-global-ip outside-local-ip [**add-route**]*.

Example 15-32 *Configuring Outside Static NAT*

```
R5# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)# interface GigabitEthernGi0/0
R5(config-if)# ip nat outside
R5(config-if)# interface GigabitEthernGi0/1
R5(config-if)# ip nat inside
R5(config-if)# exit
R5(config)# ip nat outside source static 10.123.4.2 10.123.4.222
```

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

Outside Static NAT Demonstration

R6, R7, R8, or R9 could initiate a Telnet session with R2's IP address (10.123.4.2) and no NAT translation would occur. The same routers could initiate a Telnet session with the R2's outside local IP address 10.123.4.222; or R2 could initiate a session with any of the inside hosts (R6, R7, R8, or R9) to demonstrate the outside static NAT entry.

Example 15-33 shows R2 establishing a Telnet session with R9 (10.78.9.9).

- From R9's perspective, the connection came from 10.123.4.222.
- At the same time, R8 initiated a Telnet session with the outside static NAT outside local IP address (10.123.4.222)
- From R2's perspective, the source address is R8's 10.78.9.8 IP address.

Example 15-33 *Generating Network Traffic with Outside Static NAT*

```
R2# telnet 10.78.9.9
Trying 10.78.9.9 ... Open
************************************************************
* You have remotely connected to R9 on line 2
************************************************************
User Access Verification
Password:

R9#show tcp brief
TCB        Local Address               Foreign Address             (state)
F6A23AF0   10.78.9.9.23                10.123.4.222.57126          ESTAB
```

```
R8# telnet 10.123.4.222
Trying 10.123.4.222 ... Open
************************************************************
* You have remotely connected to R2 on line 2
************************************************************
User Access Verification
Password:

R2# show tcp brief
TCB        Local Address               Foreign Address             (state)
F64C9460   10.123.4.2.57126            10.78.9.9.23                ESTAB
F64C9B60   10.123.4.2.23               10.78.9.8.11339             ESTAB
```

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

NAT Translation Table for Outside Static NAT

Figure 15-9 shows the translation table of R5 for the outside static NAT entry of R2 for 10.123.4.222.

Example 15-34 shows the NAT translation table of R5.

There are three entries:

- The first entry is the outside static NAT entry that was configured.
- The second entry is the Telnet session launched from R8 to the 10.123.4.222 IP address.
- The third entry is the Telnet session launched from R2 to R9's IP address (10.78.9.9).

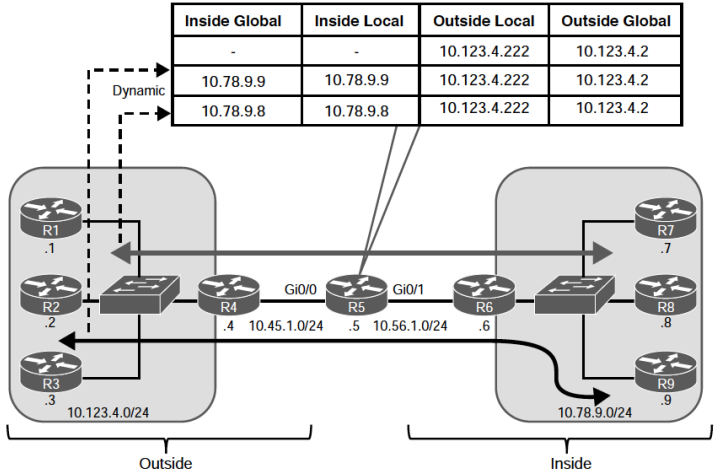

Figure 15-9 *Outside Static NAT Topology for R2 as 10.123.4.222*

Example 15-34 *NAT Translation Table for Outside Static NAT*

```
R5# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.123.4.222       10.123.4.2
tcp 10.78.9.8:11339    10.78.9.8:11339    10.123.4.222:23    10.123.4.2:23
tcp 10.78.9.9:23       10.78.9.9:23       10.123.4.222:57126 10.123.4.2:57126
```

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

Pooled NAT

A downfall to static NAT is the number of configurations entries that must be created on the NAT device. In addition, the number of global IP addresses must match the number of local IP addresses.

Pooled NAT provides a more dynamic method of providing a one-to-one IP address mapping—but on a dynamic, as-needed basis.

The dynamic NAT translation stays in the translation table until traffic flow from the local address to the global address has stopped and the timeout period (24 hours by default) has expired. The unused global IP address is then returned to the pool to be used again.

Pooled NAT can operate as inside NAT or outside NAT.

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

Pooled NAT Configuration Steps

The steps for configuring inside pooled NAT are as follows:

Step 1. Configure the outside interfaces by using the command **ip nat outside**.

Step 2. Configure the inside interface with the command **ip nat inside**.

Step 3. Specify which traffic to translate by using a standard or extended ACL referenced by number or name. Using a user-friendly name may be simplest from an operational support perspective

Step 4. Define the global pool of IP addresses by using the command **ip nat pool** *nat-pool-name starting-ip ending-ip* **prefix-length** *prefix-length*.

Step 5. Configure the inside pooled NAT by using the command **ip nat inside source list** *acl* **pool** *nat-pool-name***.**

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

Configuring Inside Pooled NAT

Example 15-35 uses a NAT pool with the IP addresses 10.45.1.10 and 10.45.1.11. A named ACL, ACL-NAT-CAPABLE, allows only packets sourced from the 10.78.9.0/24 network to be eligible for pooled NAT.

In Example 15-35, R7 and R8 ping R1 in order to generate traffic and build the dynamic inside NAT translations.

Example 15-35 *Configuring Inside Pooled NAT*

```
R5# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)# ip access-list standard ACL-NAT-CAPABLE
R5(config-std-nacl)# permit 10.78.9.0 0.0.0.255
R5(config-std-nacl)# exit
R5(config)# interface GigabitEthernGi0/0
R5(config-if)# ip nat outside
R5(config-if)# interface GigabitEthernGi0/1
R5(config-if)# ip nat inside
R5(config-if)# exit
R5(config)# ip nat pool R5-OUTSIDE-POOL 10.45.1.10 10.45.1.11 prefix-length 24
R5(config)# ip nat inside source list ACL-NAT-CAPABLE pool R5-OUTSIDE-POOL
```

Example 15-36 *Initial Traffic for Pooled NAT*

```
R7# ping 10.123.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.123.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R8# ping 10.123.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.123.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

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

Pooled NAT Table

In Example 15-37, there are a total of four translations in the translation table of R5. Two of them are for the full flow and specify the protocol, inside global, inside local, outside local, and outside global IP addresses.

In Example 15-38, R8 establishes a Telnet session with R2. R2 detects that the remote IP address of the session is 10.45.1.11. A second method of confirmation is to examine the NAT translation on R5, where there is a second dynamic translation entry for the full Telnet session.

Example 15-37 *Viewing the Pooled NAT Table for R5*

```
R5# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.45.1.10:0      10.78.9.7:0        10.123.4.1:0       10.123.4.1:0
--- 10.45.1.10         10.78.9.7          ---                ---
icmp 10.45.1.11:0      10.78.9.8:0        10.123.4.1:0       10.123.4.1:0
--- 10.45.1.11         10.78.9.8          ---                ---
```

Example 15-38 *Using the Dynamic One-to-One Mappings for Address Consistency*

```
R8# telnet 10.123.4.2
Trying 10.123.4.2 ... Open
************************************************************
* You have remotely connected to R2 on line 2
************************************************************
User Access Verification
Password:

R2# show tcp brief
TCB        Local Address               Foreign Address             (state)
F3B64440   10.123.4.2.23               10.45.1.11.34115            ESTAB
```

```
R5# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.45.1.10:1      10.78.9.7:1        10.123.4.1:1       10.123.4.1:1
--- 10.45.1.10         10.78.9.7          ---                ---
icmp 10.45.1.11:1      10.78.9.8:1        10.123.4.1:1       10.123.4.1:1
tcp 10.45.1.11:34115   10.78.9.8:34115    10.123.4.2:23      10.123.4.2:23
--- 10.45.1.11         10.78.9.8          ---                ---
```

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

Failed NAT Pool Allocation/Reset NAT Pool

A downfall to using pooled NAT is that when the pool is exhausted, no additional translation can occur until the global IP address is returned to the pool. Example 15-39 demonstrates this concept with NAT failing on R5 and packets being dropped.

The default timeout for NAT translations is 24 hours, but this can be changed with the command **ip nat translation timeout** *seconds*.

The dynamic NAT translations can be cleared out with the command **clear ip nat translation** {*ip-address* | *}, This removes all existing translations and could interrupt traffic flow on active sessions as they might be assigned new global IP addresses.

Example 15-39 *Failed NAT Pool Allocation*

```
R9# telnet 10.123.4.1
Trying 10.123.4.1 ...
% Destination unreachable; gateway or host down
```

```
R5# debug ip nat detailed
IP NAT detailed debugging is on
R5#
 02:22:58.685: NAT: failed to allocate address for 10.78.9.9, list/map
ACL-NAT-CAPABLE
 02:22:58.685:  mapping pointer available mapping:0
 02:22:58.685: NAT*: Can't create new inside entry - forced_punt_flags: 0
 02:22:58.685: NAT: failed to allocate address for 10.78.9.9, list/map ACL-NAT-CAPABLE
 02:22:58.685:  mapping pointer available mapping:0
 02:22:58.685: NAT: translation failed (A), dropping packet s=10.78.9.9 d=10.123.4.1
```

Example 15-40 *Clearing NAT Translation to Reset the NAT Pool*

```
R5# clear ip nat translation *
```

```
R9# telnet 10.123.4.1
Trying 10.123.4.1 ... Open
************************************************************
* You have remotely connected to R1 on line 2
************************************************************
User Access Verification
Password:

R1#
```

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

Port Address Translation

Pooled NAT translation has the limitation of ensuring that the number of global IP addresses is adequate to meet the needs of the local IP addresses.

Port Address Translation (PAT) is an iteration of NAT that allows for a mapping of many local IP addresses to one global IP address.

The NAT device maintains the state of translations by dynamically changing the source ports as a packet leaves the outside interface.

Another term for PAT is NAT overload.

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

Configuring PAT

The steps for configuring PAT are as follows:

Step 1. Configure the outside interface by using the command **ip nat outside**.

Step 2. Configure the inside interface with the command **ip nat inside**.

Step 3. Specify which traffic can be translated by using a standard or extended ACL referenced by number or name.

Step 4. Configure Port Address Translation by using the command **ip nat inside source list** *acl* {interface *interface-id* | pool *nat-pool-name*} **overload**.

Example 15-41 *Configuring PAT on R5*

```
R5# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)# ip access-list standard ACL-NAT-CAPABLE
R5(config-std-nacl)# permit 10.78.9.0 0.0.0.255
R5(config-std-nacl)# exit
R5(config)# interface GigabitEthernGi0/0
R5(config-if)# ip nat outside
R5(config-if)# interface GigabitEthernGi0/1
R5(config-if)# ip nat inside
R5(config)# ip nat source list ACL-NAT-CAPABLE interface GigabitEthernGi0/0 overload
```

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

Generating Traffic for PAT

Example 15-42 *Generating Network Traffic for PAT*

```
R7# ping 10.123.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.123.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R8# ping 10.123.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.123.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R9# ping 10.123.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.123.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R7# telnet 10.123.4.2
Trying 10.123.4.2 ... Open
************************************************************
* You have remotely connected to R2 on line 2
************************************************************
User Access Verification
Password:

R2# show tcp brief
TCB        Local Address               Foreign Address             (state)
F3B64440   10.123.4.2.23               10.45.1.5.51576             ESTAB
```

Now that PAT has been configured on R5, traffic can be generated for testing.

```
R8# telnet 10.123.4.2
Trying 10.123.4.2 ... Open
************************************************************
* You have remotely connected to R2 on line 3
************************************************************
User Access Verification
Password:

R2# show tcp brief
TCB        Local Address               Foreign Address             (state)
F3B64440   10.123.4.2.23               10.45.1.5.51576             ESTAB
F3B65560   10.123.4.2.23               10.45.1.5.31515             ESTAB
```

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

NAT Translation Table With PAT

Figure 15-10 shows R5's translation table after all the various flows have established.

Example 15-43 shows R5's NAT translation table. By taking the ports from the TCP brief sessions on R2 and correlating them to R5's NAT translation table, you can identify which TCP session belongs to R7 or R8.

Inside Global	Inside Local	Outside Local	Outside Global
10.45.1.5:4	10.78.9.7:3	10.123.4.1:3	10.123.4.1:4
10.45.1.5:3	10.78.9.8:3	10.123.4.1:3	10.123.4.1:3
10.45.1.5:1	10.78.9.9:1	10.123.4.1:1	10.123.4.1:1
10.45.1.5:51576	10.78.9.7:51576	10.123.4.2:23	10.123.4.2:23
10.45.1.5:31515	10.78.9.8:31515	10.123.4.2:23	10.123.4.2:23

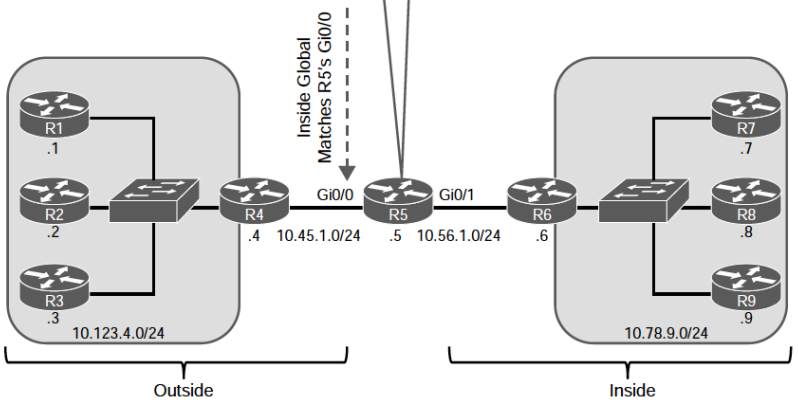

Figure 15-10 *R5's Translation Table for PAT*

Example 15-43 *R5's NAT Translation Table with PAT*

```
R5# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.45.1.5:4       10.78.9.7:3        10.123.4.1:3       10.123.4.1:4
icmp 10.45.1.5:3       10.78.9.8:3        10.123.4.1:3       10.123.4.1:3
icmp 10.45.1.5:1       10.78.9.9:1        10.123.4.1:1       10.123.4.1:1
tcp 10.45.1.5:51576    10.78.9.7:51576    10.123.4.2:23      10.123.4.2:23
tcp 10.45.1.5:31515    10.78.9.8:31515    10.123.4.2:23      10.123.4.2:23
```

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

Prepare for the Exam

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

Prepare for the Exam

Key Topics for Chapter 15

Description
Network Time Protocol
NTP stratums
Stratum preferences
NTP peers
First-hop redundancy protocol (FHRP)
Hot Standby Router Protocol (HSRP)
HSRP configuration
HSRP object tracking
Virtual Router Redundancy Protocol
Legacy VRRP configuration

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

Key Topics for Chapter 15 (Cont.)

Description	
Hierarchical VRRP configuration	Viewing the NAT translation table
Global Load Balancing Protocol	NAT processing
GLBP configuration	Outside static NAT configuration
GLBP load-balancing options	Pooled NAT configuration
NAT terms	NAT timeout
Common NAT types	Port Address Translation (PAT)
Inside static NAT configuration	PAT configuration

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

Prepare for the Exam

Key Terms for Chapter 15

Terms	
First-hop redundancy protocol	Outside local
Inside global	Outside global
Inside local	Pooled NAT
Network Address Translation (NAT)	Port Address Translation (PAT)
NTP client	Static NAT
NTP peer	stratum
NTP Server	

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

Command Reference for Chapter 15

Task	Command Syntax
Configure a device as an NTP client with the IP address of the NTP server	**ntp server** *ip-address* [**prefer**] [**source** *interface-id*]
Configure a device so that it can respond authoritatively to NTP requests when it does not have access to an atomic clock or an upstream NTP server	**ntp master** *stratum-number*
Configure the peering with another device with NTP	**ntp peer** *ip-address*
Configure the tracking of an interface's line protocol state	**track** *object-number* **interface** *interface-id* **line-protocol**
Configure a device to track the installation of a route in the routing table	**track** *object-number* **ip route** *route/ prefix-length* **reachability**
Configure the VIP for the HSRP instance	**standby** *instance-id* **ip** *vip-address*
Enable preemption for the HSRP instance	**standby** *instance-id* **preempt**

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

Command Reference for Chapter 15 (Cont.)

Task	Command Syntax
Specify the MAC address for the HSRP VIP	**standby** *instance-id* **mac-address** *mac-address*
Configure the HSRP timers for neighbor health checks	**standby** *instance-id* **timers** {**seconds** | **msec milliseconds**}
Link object tracking to a decrease in priority upon failure of the HSRP	**standby** *instance-id* **track** *object-id* **decrement** *decrement-value*
Configure the VIP gateway for the VRRP instance	**vrrp** *instance-id* **ip** *vip-address*
Configure the priority for the VRRP instance	**vrrp** *instance-id* **priority**
Link object tracking to a decrease in priority upon failure with VRRP	**vrrp** *instance-id* **track** *object-id* **decrement** *decrement-value*
Configure the VIP gateway for a GLBP instance	**glbp** *instance-id* **ip** *vip-address*
Enable preemption for a GLBP instance	**glbp** *instance-id* **preempt**

Command Reference for Chapter 15 (Cont.)

Task	Command Syntax
Configure the priority for a GLBP instance	**glbp** *instance-id* **priority** *priority*
Configure GLBP timers for neighbor health checks	**glbp** *instance-id* **timers** {*hello-seconds* | **msec** *hello-milliseconds}* {*hold- seconds* | **msec** *hold-milliseconds*}
Configure the GLBP load-balancing algorithm	**glbp** *instance-id* **load-balancing** {**host-dependent** | **round-robin** | **weighted**}.
Configure the devices GLBP weight for traffic load balancing	**glbp** *instance-id* **weighting** *weight*
Configure an interface as an outside interface for NAT	**ip nat outside**
Configure an interface as an inside interface for NAT	**ip nat inside**
Configure static inside NAT	**ip nat inside source static** *inside- local-ip inside-global-ip*

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

Command Reference for Chapter 15 (Cont.)

Task	Command Syntax
Configure static outside NAT	**ip nat outside source static** *outside- global-ip outside-local-ip* [**add-route**]
Configure pooled NAT	**ip nat pool** *nat-pool-name starting-ip ending-ip* **prefix-length** *prefix-length*
Define the NAT pool for global IP addresses	**ip nat inside source list** *acl* **pool** *nat-pool-name*
Configure a device for PAT	**ip nat inside source list** *acl* {**interface** *interface-id* | **pool** *nat-pool-name*} **overload**
Modify the NAT timeout period	**ip nat translation timeout** *seconds*
Clear a dynamic NAT entry	**clear ip nat translation** *{ip-address* | ***}*
Display the status of the NTP service, hardware clock synchronization status, reference time, and time since last polling cycle	**show ntp status**

Command Reference for Chapter 15 (Cont.)

Task	Command Syntax
Display the list of configured NTP servers and peers and their time offset from the local device	**show ntp associations**
Display the status of a tracked object	**show track** [*object-number*]
Display the status of an HSRP VIP	**show standby** [*interface-id*] [**brief**]
Display the status of a VRRP VIP	**show vrrp** [**brief**]
Display the status of a GLBP VIP	**show glbp** [**brief**]
Display the translation table on a NAT device	**show ip nat translations**

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


CISCO