# IPv6 Network Management

Andy Chien (錢小山)

Customer Solutions Architect

Cisco Systems

Dec-07-2012

© 2010 Cisco and/or its affiliates. All rights reserved.

# Agenda

- SNMP
  - SNMP over IPv6
  - MIB Updates
  - Troubleshooting, caveats and bugs
- IPSLA and IPv6
- DNS and IPv6
- DHCPv6
- Other Management Protocols and Instrumentations
  - HTTP, Syslog, Netflow, Telnet, SSH, CDP, ping , traceroute
  - EEM, ESM, Tcl

© 2010 Cisco and/or its affiliates. All rights reserved.

# SNMP over IPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# SNMP over IPv6

- **SNMP is an application Layer Protocol**
  - **IPv6 is just another Network Layer Protocol for SNMP**
  - **Easy Enough!!**
- Works out of the box as long as IPv6 is enabled on the device
- SNMP still uses UDP at Layer 4
- SNMP uses UDP Port 161 for polling and UDP Port 162 for traps – same as for IPv4
- No problems in SNMP itself as the protocol remains the same
  - Problems lie in the MIBs and in the lack of support for IPv6 in various MIBs

© 2010 Cisco and/or its affiliates. All rights reserved.

# SNMP over IPv6 Example

- IPv4

```
#snmpwalk -v 2c -c public 172.16.174.54 1.3.6.1.2.1.1.5
iso.3.6.1.2.1.1.5.0 = STRING: "NMS-2911-A.cisco.com”
```

- IPv6

```
#snmpwalk -v 2c -c public udp6:[fec0::54] 1.3.6.1.2.1.1.5
iso.3.6.1.2.1.1.5.0 = STRING: "NMS-2911-A.cisco.com”
```

- IOS Configuration for sending SNMP Traps over IPv6

```
snmp-server host 2001:12::1 version 2c public
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# Why do MIBs matter for IPv6?

- MIBs define the objects that can be polled using SNMP
- Most MIBs need to be updated to support IPv6
- Problems in MIBs manifest in two ways
  - Support for IPv4 only as some MIBs use the legacy ipAddress type, which cannot hold an IPv6 address
  - IPv4 addresses embedded in OIDs, data
- **These issues can be resolved in two ways**
  - **New MIBs can be created – IPv6 only or Protocol Independent**
  - **Existing MIBs can be modified to add new OIDs to support IPv6**
- Still a lot of work remains to be done

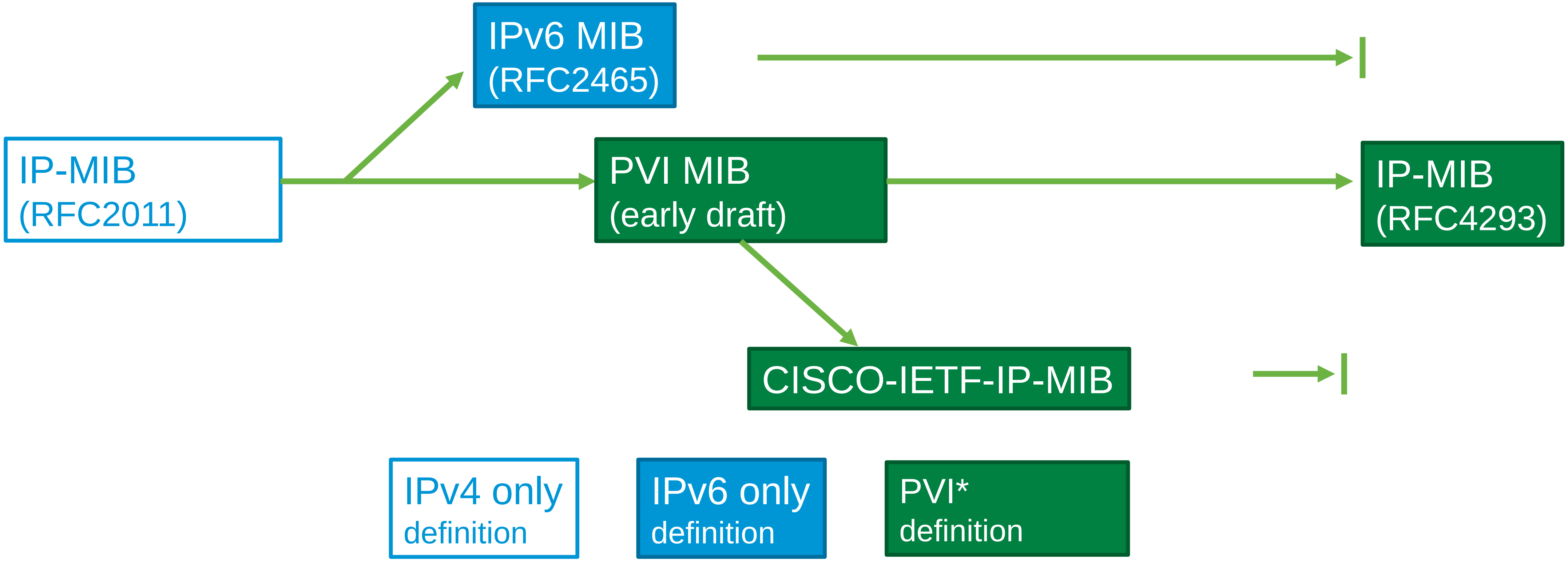
© 2010 Cisco and/or its affiliates. All rights reserved.

# IP-MIB and IP-FORWARD-MIB

- Basic IETF MIBs defined in RFCs
- Provide details such as
  - IP Addresses configured on a device
  - IP Address to Data Link Layer Mappings
  - The IP Routing Table
- **Latest definitions available in**
  - **RFC 4293 – IP-MIB**
  - **RFC 4292 – IP-FORWARD-MIB**
- The next few slides show evolution of these MIBs

© 2010 Cisco and/or its affiliates. All rights reserved.

# IETF Modifications (IP-MIB)




*PVI – Protocol Version Independent

- This chart shows the IP-MIB developments
- There are similar developments for the IP-FORWARD-MIB

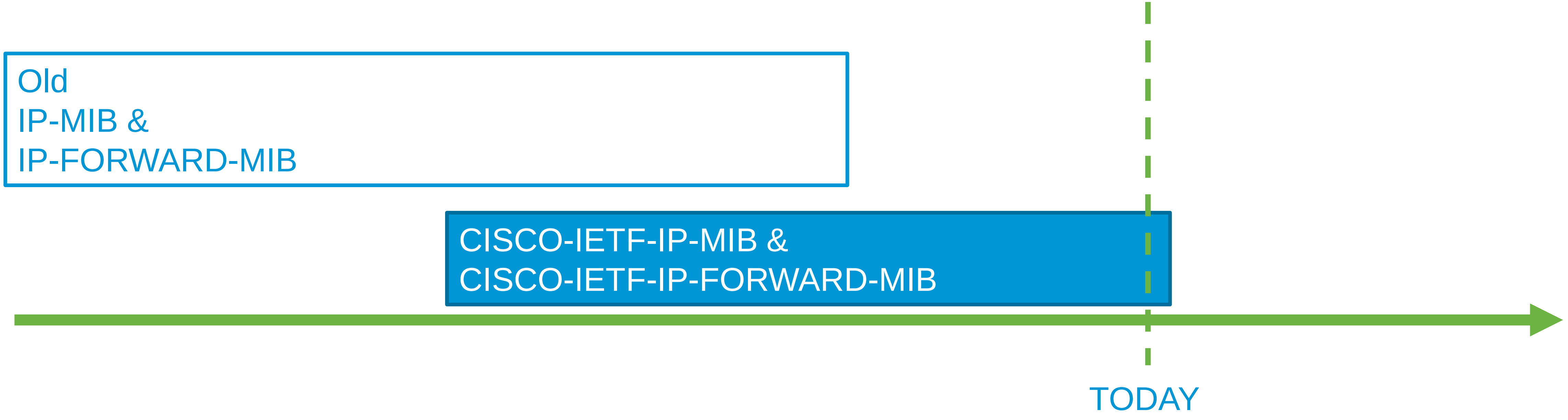
© 2010 Cisco and/or its affiliates. All rights reserved.

# Cisco IOS MIB Support


- Cisco IOS Software has supported the ‘IP-MIB’ and the ‘IP-FORWARD-MIB’ for a long time
- Most IOS versions today support RFC1213 and RFC2096 respectively
- These revisions of the MIBs are IPv4 only

© 2010 Cisco and/or its affiliates. All rights reserved.

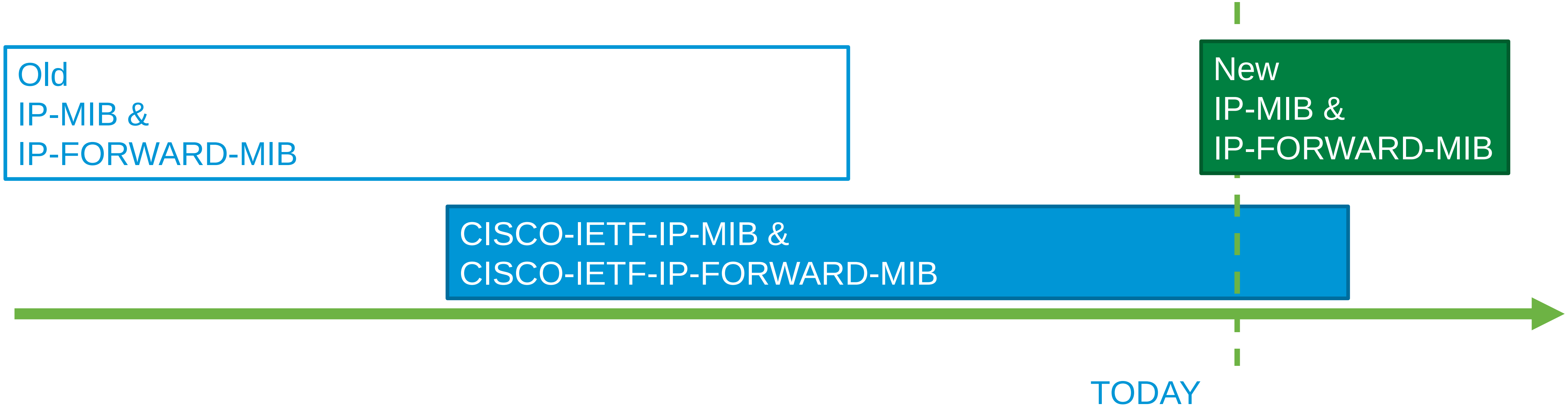
# Cisco IOS MIB Support




- In 2003, IOS introduced the CISCO-IETF-IP-MIB and CISCO-IETF-IP-FORWARD-MIB
- These are based on the IETF draft-ietf-ipngwg-rfc[2011|2096] IDs
- The definitions are protocol version independent, but the IOS implementation is for IPv6 objects/tables only

© 2010 Cisco and/or its affiliates. All rights reserved.

# Cisco IOS MIB Support




- The final aim is to implement new definitions of the IP-MIB and IP-FORWARD-MIB
- Use the PVI tables in the new definitions of both MIBs for both IPv4 and IPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# Important PI Tables RFC 4292/93

- ipAddressTable - IP Address Information
- ipSystemStatsTable – System wide stats
- ipIfStatsTable – Interface specific stats
- inetCidrRouteTable – Routing Table

Sample snmpwalk's of these tables done on 15.1(4)M are available at http://foosball.cisco.com/publish/rfc-4292-4293-walks.tar.gz

© 2010 Cisco and/or its affiliates. All rights reserved.

# MIB Revisions

- MIBs can be changed, In fact, many MIBs get updated regularly
  - New objects are added
  - Old objects are deprecated – not removed
- For every set of changes in the MIB,
  - New MIB Revision Number is defined
  - Details on the objects added/deprecated is provided in the MIB
- **To support IPv6 functionality, objects may be added to existing MIBs**
  - **e.g. ‘ipAddress’ objects might be deprecated and instead ‘inetAddressType’ and ‘inetAddress’ objects added in its place.**

© 2010 Cisco and/or its affiliates. All rights reserved.

# MIB Revisions

- Example of CISCO-FLASH-MIB Revisions

```
REVISION        "200501280000Z"
    DESCRIPTION
        "Added a new status copyOperationPending(0)
        to object ciscoFlashCopyStatus.”


REVISION        "200403180000Z"
    DESCRIPTION
        "The object ciscoFlashCopyServerAddress is
        deprecated since it supports only IPv4 address. Two
        new objects ciscoFlashCopyServerAddrRev1
        ciscoFlashCopyServerAddrType are defined.”
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# MIB Revisions

- So how would you know what MIB revision is bundled with a particular IOS version?
- MIB Names remain the same even if revision number changes
- It's a painful process to find MIB revision numbers in IOS
  - Not accessible through CLI or SNMP (CSCtn03463)
  - No external Tool
  - Use http://nm-tac.cisco.com/search/mii/ to enter IOS image name and get revision of the MIB bundled with that IOS
- Why is this a problem?
  - If you do not know the MIB revision, you may be polling/setting the incorrect objects.
  - Examples of a MIB revision problem – 617146391, 609886499, 611381783

© 2010 Cisco and/or its affiliates. All rights reserved.

# MIB Revisions

| IOS | MIB | Revision |
|---|---|---|
| c2900-universalk9-mz.SPA.151-3.T | CISCO-WAN-3G-MIB | 201008110000Z |
| c2900-universalk9-mz.SPA.150-1.M4 | CISCO-WAN-3G-MIB | 200902050000Z |

© 2010 Cisco and/or its affiliates. All rights reserved.

# Troubleshooting

- Debugging for SNMP is the same in IPv6 as it was in IPv4
- Show commands
  show run | in snmp-server
  show snmp
  show snmp user
  show snmp group
- Debug commands
  debug snmp packets
  debug snmp headers
  debug snmp detail
- Packet captures are great to troubleshoot SNMP Issues
  **Install MIBs on wireshark to decode and map numeric OIDs to names**

Note - Recent versions of wireshark do not allow adding MIB, so you may need to use older versions

© 2010 Cisco and/or its affiliates. All rights reserved.

# Troubleshooting

- For problems with high CPU utilization or tracebacks, you can gather the following information
- Stack Trace of the SNMP Engine Process
  - Get the ‘show version’ output
  - Get the PID using ‘show proc cpu | in SNMP ENGINE
  - Get the stack trace using ‘show stack <PID>
  - A stack trace of more than 4 lines usually signifies some activity
  - It is always a good idea to get multiple stack traces to capture the issue
  - Decode the stack trace using ‘rsym’
- Newer IOS versions have a command to show recently polled OIDs – show snmp stats oid
- Apply a SNMP view to restrict polling for problematic MIBs

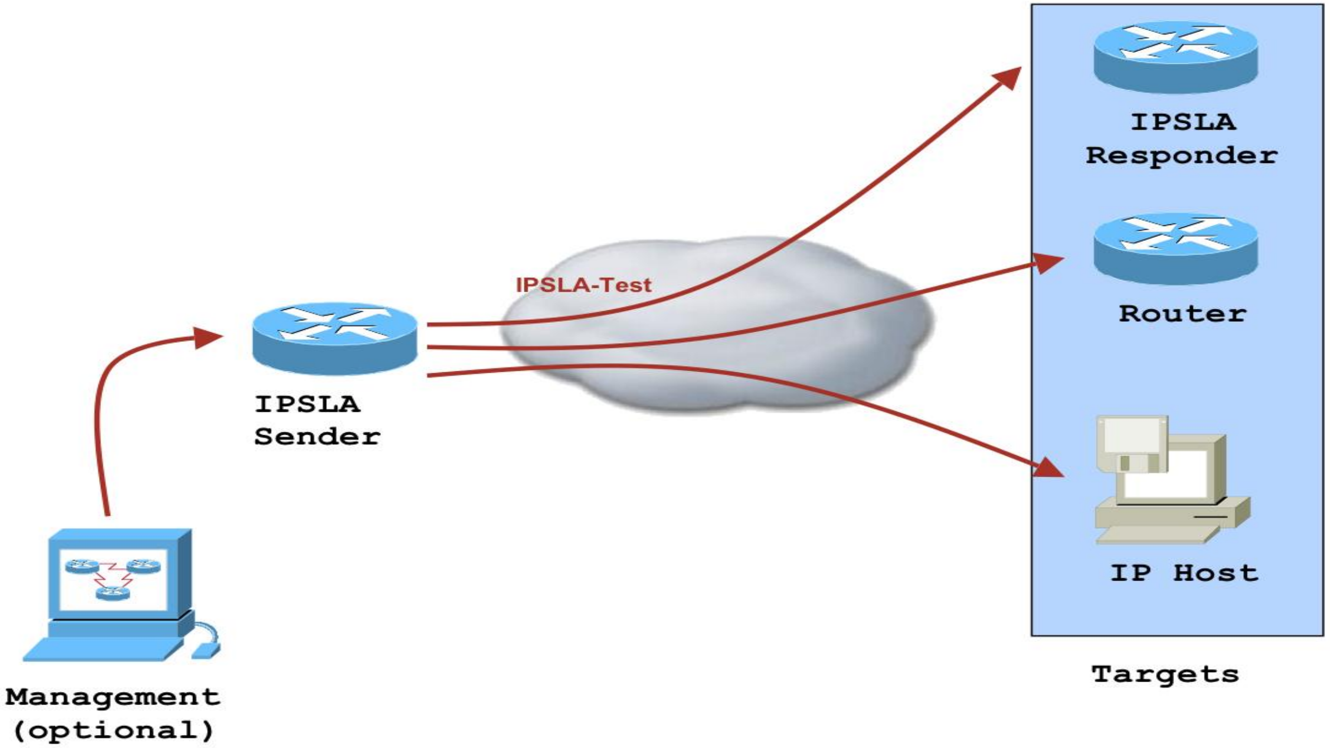
© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA and IPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA – Some background

- Cisco IOS IP Service Level Agreements (SLAs) are a portfolio of technology embedded in most devices that run Cisco IOS software that allow Cisco customers to analyse service levels for IP applications and services
- IP SLA uses active traffic monitoring - the generation of traffic in a continuous, reliable, and predictable manner - for measuring network performance
- Initially called ‘Response Time Reporter (RTR)’, then renamed to Service Assurance Agent (SAA), the feature is now called IP Service Level Agreement (IPSLA)




For more info:
http://wwwin.cisco.com/ios/tech/mgmt/ipsla/
http://www.cisco.com/go/ipsla

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA – IPv4 and IPv6 Comparison

- So what is the scope of the IPv6 IPSLA discussion?
- IP SLA probes over an IPv6 transport
- Using SNMP set over v4/v6 transport to create v6 probes

| Operation Type | IPv4 | IPv6 |
|---|---|---|
| ICMP echo | YES | YES |
| ICMP jitter | YES | |
| ICMP path echo | YES | |
| ICMP path jitter | YES | |
| UDP echo | YES | YES |
| UDP jitter | YES | YES |
| UDP jitter for VoIP | YES | |
| DLSw+ | YES | |
| DNS | YES | |
| DHCP | YES | |
| FTP | YES | |
| HTTP | YES | |
| RTP-based VoIP | YES | |
| TCP connect | YES | YES |
| VoIP gatekeeper registration delay | YES | |
| VoIP post-dial delay | YES | |

Current workaround for lack of IPv6 operation types:
IPv4 IPSLA probes in an IPv4 over IPv6 tunnel

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA – Supported IOS versions

- **Verify if the router image supports both IP SLAs and IPv6**
- IOS Versions implementing Licensing require a data/uc/security license to configure device as a IP SLA source
- In older IOS versions, the ipbase feature set may not support IPSLA
- IPv6 Support for ICMP Echo, UDP Echo, UDP Jitter and TCP Connect

  12.2(50)SY

  12.2(33)SRC

  12.2(33)SB

  12.4(20)T

  IOS XE 3.1.0SG
- Use Cisco Feature navigator to find Supported IP SLA Features

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA – IPv6 Pre-requisites

- Enable IPv6 Routing and configure IPv6 Address
- By default, IPv6 routing is disabled in the Cisco IOS software. To enable IPv6 routing, you must first enable the forwarding of IPv6 traffic globally on the router and then you must assign IPv6 addresses to individual interfaces in the router

```
Router(config)#ipv6 unicast-routing
Router(config)#interface Ethernet0
Router(config-if)#ipv6 address 2001:12::1/64
```

Note: At least one interface must be configured with an IPv6 address before configuring the IPv6 options in IP SLA

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA – Configuring IPSLA Operations

- When at least one IPv6 address is configured, the IPv6 options of IP SLA will become available.

```
Router(config)# ip sla 1
Router(config-ip-sla)# udp-jitter ?
   Hostname or X:X:X:X::X
   Hostname or A.B.C.D Destination IP/IPv6 address or hostname
```

- All the operations are entirely identical to their IPv4 equivalent, and are configured in exactly the same way. There is no functional, performance, scalability or accuracy difference between IPv4 and IPv6

- Some operations such as UDP Echo and UDP Jitter will require a responder. The responder is configured the same way as with IPv4:

```
Router(config)# ip sla responder
```

Note: The responder is automatically enabled for both IPv4 and IPv6. There is no option to enable it only for one protocol, but this can still be done with access-lists.

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA - Examples

- Configuration example of an ICMP Echo operation

```
ip sla 1
   icmp-echo 2001::214:A8FF:FE7A:ED70
ip sla schedule 1 start-time now
```

- Configuration example of a TCP connect operation

```
ip sla 2
   tcp-connect 2001::214:A8FF:FE7A:ED70 5566
ip sla schedule 2 start-time now
```

- Configuration example of an UDP Echo operation

```
ip sla 3
   udp-echo 2001::214:A8FF:FE7A:ED70 5566
ip sla schedule 3 start-time now
```

- Configuration example of a UDP Jitter operation

```
ip sla 4
   udp-jitter 2001::214:A8FF:FE7A:ED70 5566
ip sla schedule 4 start-time now
```

```
Router(config)# ip sla responder
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA MIBs

- IP SLA Operations can be created/edited/deleted using SNMP
- CISCO-RTTMON-MIB is the primary MIB used
- Configurations created using SNMP may or may not show up in the running config – depends on the rttMonCtrlAdminNvgen flag
- **'show ip sla configurations' always shows all the operations configured**
- To support, IPv6, the CISCO-RTTMON-IP-EXT-MIB was introduced

  crttMonIPEchoAdminTargetAddrType and crttMonIPEchoAdminTargetAddress

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA – IPv6 Configuration using SNMP

```
#snmpset -M ~/mibs -m CISCO-RTTMON-MIB:CISCO-RTTMON-IP-EXT-MIB -v2c -c private 172.16.174.54 \
rttMonCtrlAdminStatus.1 i 4 \
rttMonCtrlAdminRttType.1 i 6 \
rttMonEchoAdminProtocol.1 i 24 \
rttMonCtrlAdminNvgen.1 i 1 \
rttMonEchoAdminTargetPort.1 i 23 \
crttMonIPEchoAdminTargetAddrType.1 i 2 \
crttMonIPEchoAdminTargetAddress.1 s \ "20:01:00:12:00:00:00:00:00:00:00:00:00:00:00:02"

CISCO-RTTMON-MIB::rttMonCtrlAdminStatus.1 = INTEGER: createAndGo(4)
CISCO-RTTMON-MIB::rttMonCtrlAdminRttType.1 = INTEGER: tcpConnect(6)
CISCO-RTTMON-MIB::rttMonEchoAdminProtocol.1 = INTEGER: ipTcpConn(24)
CISCO-RTTMON-MIB::rttMonCtrlAdminNvgen.1 = INTEGER: true(1)
CISCO-RTTMON-MIB::rttMonEchoAdminTargetPort.1 = INTEGER: 23
CISCO-RTTMON-IP-EXT-MIB::crttMonIPEchoAdminTargetAddrType.1 = INTEGER: ipv6(2)
CISCO-RTTMON-IP-EXT-MIB::crttMonIPEchoAdminTargetAddress.1 = STRING:
"20:01:00:12:00:00:00:00:00:00:00:00:00:00:00:02"

ip sla 1
 tcp-connect 3131:3A32:333A:3435:3A36:373A:3030:3A30 23
```

Caveat:
Currently being
investigated

© 2010 Cisco and/or its affiliates. All rights reserved.

# IP SLA – Notes and Caveats

- Performance numbers might be slightly less accurate with IPv6 tests, primarily because the IPv4 microseconds timestamps cannot be used for IPv6 (at the moment). This problem affects both the sender and responder. CSCtd50484 and CSCte00862 are tracking these issues
- VRF-aware operations over IPv6 are not supported. Some IOS versions allow it to be configured but should not (CSCsq08526)
- Auto IP SLAs and auto-registration do not support IPv6
- Multicast or anycast addresses are not supported
- There are some funny bugs - CSCsv51014
  - Control packet uses ipv6 address on 1st try, ipv4 on 2nd and 3rd try ☺
- Some caveats affecting probes created by SNMP - CSCsv77030
- And, there are some more we haven't found yet!!

© 2010 Cisco and/or its affiliates. All rights reserved.

# DNS and IPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# DNS Requirements for IPv6

- With IPv6, you network will have  both IPv4 and IPv6 addresses. Therefore, you need to add mappings from names to IPv6 addresses in parallel with the existing mapping from names to IPv4 addresses
- To support IPv6 addresses, DNS Servers now need to support AAAA records – pronounced quad-A
- DNS Servers also need to map IPv6 addresses back to names. This is done using reverse DNS lookups in the ip6.arpa domain
- **DNS servers must be able to respond to requests coming in over IPv4 or IPv6**
- **DNS Servers must be able to talk to other DNS server (forwarding, recursion, zone transfers) over both IPv4 and IPv6**

© 2010 Cisco and/or its affiliates. All rights reserved.

# AAAA Resource Records

- AAAA records map the hostnames to IPv6 addresses
  - They serve the same purpose as A records for IPv4
- A sample AAAA record for a web server would look like
  - Type – AAAA
  - Name - www
  - TTL - 24h
  - Data – 2001:12::1

© 2010 Cisco and/or its affiliates. All rights reserved.

# Sample DNS Query - AAAA

```
# dig AAAA @menaces www.lab.nms.com

; <<>> DiG 9.6.0-APPLE-P2 <<>> AAAA @menaces www.lab.nms.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61871
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.lab.nms.com.     IN   AAAA

;; ANSWER SECTION:
www.lab.nms.com. 86400    IN   AAAA    2001:12::1

;; AUTHORITY SECTION:
lab.nms.com.      86400    IN   NS   mobeius.lab.nms.com.

;; Query time: 1 msec
;; SERVER: 172.16.174.82#53(172.16.174.82)
;; WHEN: Mon Feb 21 15:36:25 2011
;; MSG SIZE  rcvd: 94
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# ip6.arpa. Domain for PTR records

- The ip6.arpa. Domain is used for IPv6 address to hostname mappings using the PTR records
- IPv6 and IPv4 share the same record type, PTR, for reverse zones
- The PTR record in IPv6 is broken into 32 4-bit nibbles separated by the '.' symbol
- e.g. of a PTR record for the IP Address 2001:12::1

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.0.0.1.0.0.2.ip6.arpa.

© 2010 Cisco and/or its affiliates. All rights reserved.

# Sample DNS Query - PTR

```
# dig @menaces -x 2001:12::1

; <<>> DiG 9.6.0-APPLE-P2 <<>> @menaces -x 2001:12::1
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50061
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.0.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.0.0.1.0.0.2.ip6.arpa. 86400   IN PTR www.lab.nms.com.

;; AUTHORITY SECTION:
0.0.0.0.0.0.0.0.2.1.0.0.1.0.0.2.ip6.arpa. 86400 IN NS ns.lab.nms.com.

;; Query time: 11 msec
;; SERVER: 172.16.174.82#53(172.16.174.82)
;; WHEN: Mon Feb 21 15:35:07 2011
;; MSG SIZE  rcvd: 176
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# Points to Note

- The DNS protocol works at the Application Layer
  - The protocol itself – packet formats and messages – was not modified to support IPv6
  - Only changes were to addition of AAAA RR type and the introduction of the ip6.arpa. domain
- DNS queries from clients can be received over IPv4 or IPv6
  - The queries themselves can ask for A(IPv4) or AAAA(IPv6) records
- Therefore,
  - To reach a IPv6 web server from a IPv6 enabled client, the DNS Server does not need IPv6 connectivity.
  - Client sends query for AAAA record over IPv4 to DNS Server, gets the IPv6 address of the web server and connects to it over IPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# Steps to get your DNS ready for IPv6

- Setup the DNS Server to start serving AAAA records
- Setup the DNS Server to start serving ip6.arpa PTR records
- Enable IPv6 connectivity to the DNS Server, so clients can send DNS queries to the DNS Server over IPv6
- Make sure your DNS Server can forward queries and perform zone transfers over IPv6
- Add a AAAA glue record for your nameserver to the TLD zone of your domain
- Test DNS over IPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# Additional Considerations

- Be very careful when enabling DNS over IPv6 in your network
- Serving AAAA records can create problems
  - If client's IPv6 connectivity is broken
- Happy Eyeballs
- DNS Whitelisting
- World IPv6 Day – 8th Jun 2011
  - Participating organizations will serve AAAA records for their web servers
  - More Info - http://isoc.org/wp/worldipv6day/

© 2010 Cisco and/or its affiliates. All rights reserved.

# Cisco Network Registrar (CNR)

- CNR is Cisco's DHCP/DNS Server
  - It supports IPv6 starting with version 7.x
  - It can respond to clients over IPv6
  - But it cannot initiate queries over IPv6, so it cannot talk to root or other authoritative DNS servers over IPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# CNR – Other Considerations

- By default, CNR DNS server listens to all interface on a server for both IPv4 and IPv6
  - No special configuration is required, unless you want to restrict operation to a specific interface
- You may need to tweak your firewall rules to allows DNS packets larger than 512 bytes
- CNR only supports IPv4 root hints in the current version
- Zone transfers are only supported over IPv4
- Feature such as high availability, resolution exceptions, forwarding are only supported over IPv4

© 2010 Cisco and/or its affiliates. All rights reserved.

# DHCPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# DHCPv6 Basics

- Hosts use DHCPv6 to get,
  - One or more IPv6 addresses
  - One or more IPv6 prefixes
  - Configuration information using options
- Components of DHCPv6
  - DHCPv6 Clients
  - DHCPv6 Servers
  - DHCPv6 Relay Agents
- Different ways to get IPv6 addresses and/or configuration information
  - Static Configuration
  - Stateful DHCPv6
  - Stateless DHCPv6
  - Stateless Address Auto-configuration - SLACC

© 2010 Cisco and/or its affiliates. All rights reserved.

# Overview of DHCPv6

- Similar to DHCPv4 but a different protocol altogether
- Uses IPv6 transport
- DHCPv6 clients listen on port 546
- Servers and relays listen on port 547
- Operates solely at Layer 3 of the TCP/IP stack
- DHCPv6 clients and servers/relay agents communicate via link-local multicast addresses

  FF02::1:2 = All_DHCP_Relay_Agents_and_Servers

  FF05::1:3 = All_DHCP_Servers multicast address
- Relays may forward DHCPv6 messages to other relays or server using link-local multicast or global unicast IPv6 addresses

© 2010 Cisco and/or its affiliates. All rights reserved.

# DHCPv4 and DHCPv6 Comparison

| DHCP Messages | IPv4 | IPv6 | |
|---|---|---|---|
| Initial Message Exchange | 4-way handshake | 4-way handshake | 2-way handshake |
| Message Types | Broadcast, Unicast | **Multicast**, Unicast | **Multicast**, Unicast |
| Client → Server | DISCOVER | SOLICIT | SOLICIT |
| Server → Client | OFFER | ADVERTISE | REPLY |
| Client → Server | REQUEST | REQUEST | |
| Server → Client | ACK | REPLY | |

Called
Rapid Commit


© 2010 Cisco and/or its affiliates. All rights reserved.

# DHCPv4 and DHCPv6 Message types

| DHCPv4 | DHCPv6 |
| --- | --- |
| DHCPDISCOVER | SOLICIT |
| DHCPOFFER | ADVERTISE |
| DHCPREQUEST | REQUEST, RENEW, REBIND |
| DHCPACK/DHCPNAK | REPLY |
| DHCPRELEASE | RELEASE |
| DHCPINFORM | INFORMATION-REQUEST |
| DHCPDECLINE | DECLINE |
| - | CONFIRM |
| DHCPFORCERENEW | RECONFIGURE |
| - | REPAY-FORW, RELAY-REPLY |

© 2010 Cisco and/or its affiliates. All rights reserved.

# Stateless vs Stateful DHCPv6

- Stateless DHCPv6
  - DHCPv6 Server only provides configuration information
  - Two Messages are used - INFORMATION-REQUEST, REPLY
  - Assumption: Client will acquire IPv6 address through some other means (static, auto-config)

- Stateful DHCPv6
  - A DHCPv6 server will allocate one or more IPv6 addresses or prefixes to a DHCPv6 client
  - DHCPv6 options such as DNS Server, domain name may be offered to the client
  - DHCPv6 Server mains state - stores the leased IPv6 addresses and lease details in its database

© 2010 Cisco and/or its affiliates. All rights reserved.

# Role of a Router

- Routers send out periodic Router Advertisement Messages
- Prefix information or information about prefixes that are in use or valid for the link
- Router Advertisement messages include flags to control DHCPv6 behavior
  - **Managed bit to indicate use of stateful DHCPv6 – RFC 4861**
  - **Other bit to indicate use of stateless DHCPv6 – RFC 4861**
  - **The 'autonomous address-configuration flag' to indicate use of stateless address autoconfiguration – RFC 4862**
- These flags are used by the client to "decide" the use of the appropriate address assignment options
  - Note: **Exact client behavior may vary between implementations**

© 2010 Cisco and/or its affiliates. All rights reserved.

# Autonomous address-configuration flag

- Neighbor Discovery messages include 0 or more options
- Specifically option 3 – the prefix information – contains the ‘Autonomous address-configuration’ flag (A flag)
- When set, the flag indicates that the prefix specified in the prefix information option *can* be used for stateless address configuration
  - The prefix information option also includes information such as the valid lifetime and preferred lifetime of the prefix and the actual prefix
- The host uses the information in the Router Advertisement messages to autonomously configure the IP address information

© 2010 Cisco and/or its affiliates. All rights reserved.

# What do the M and O bits mean?

- M-bit

  The M bit stands for the ‘Managed Address Configuration Flag’

  When set it indicates that addresses are available via DHCPv6

  If M bit is set, the O bit can be ignored because DHCPv6 will provide all the configuration information

- O-bit

  The O bit stands for the ‘Other Configuration Flag’

  When set, the O bit indicates that other configuration information is available via the DHCPv6 server. e.g. DNS servers, domain name etc

When neither M or O bit are set, it indicates that no information is available via DHCPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# Bit Combinations – What do they mean?

| M bit | O bit | A bit | Prefix | Host Address | Other Config/Options |
|---|---|---|---|---|---|
| 0 | 0 | 0 | Static | | Manual |
| 0 | 0 | 1 | RA Message | Autonomous | Manual |
| 0 | 1 | 0 | Static | | DHCPv6 |
| 0 | 1 | 1 | RA Message | Autonomous | DHCPv6 |
| 1 | 0 | 0 | DHCPv6 (Stateful) | | DHCPv6 |
| 1 | 0 | 1 | DHCPv6 (Stateful) and/or autonomous | | DHCPv6 |
| 1 | 1 | 0 | DHCPv6 (Stateful) | | DHCPv6 |
| 1 | 1 | 1 | DHCPv6 (Stateful) and/or autonomous | | DHCPv6 |

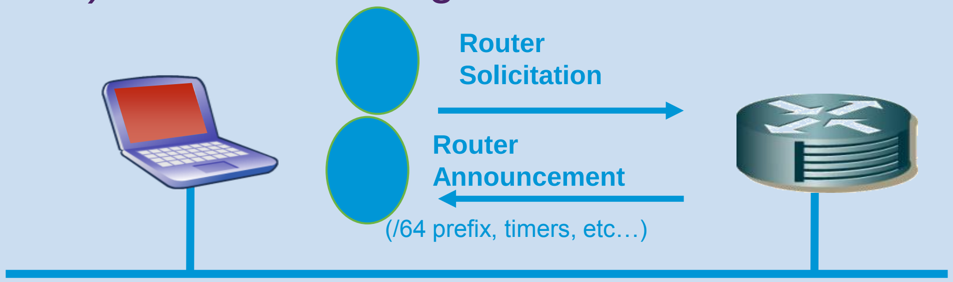
© 2010 Cisco and/or its affiliates. All rights reserved.

# IPv6 Address Assignment

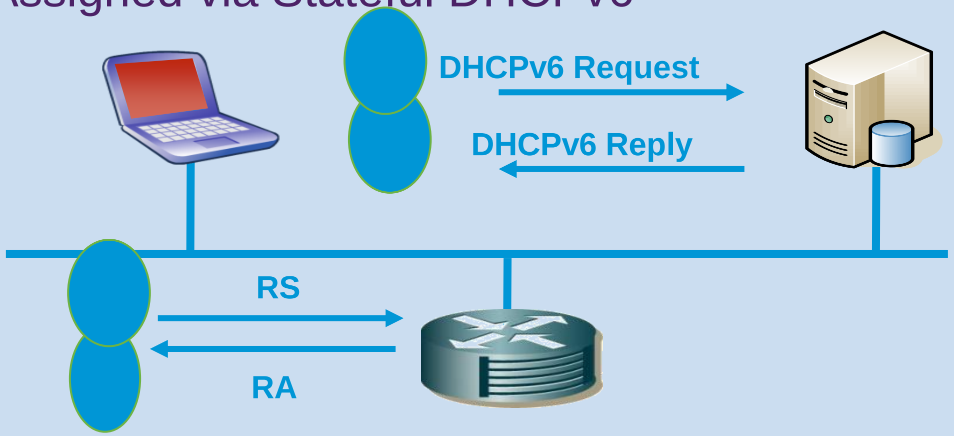
| Similar to IPv4 | New in IPv6 |
|---|---|

A) Manually configured

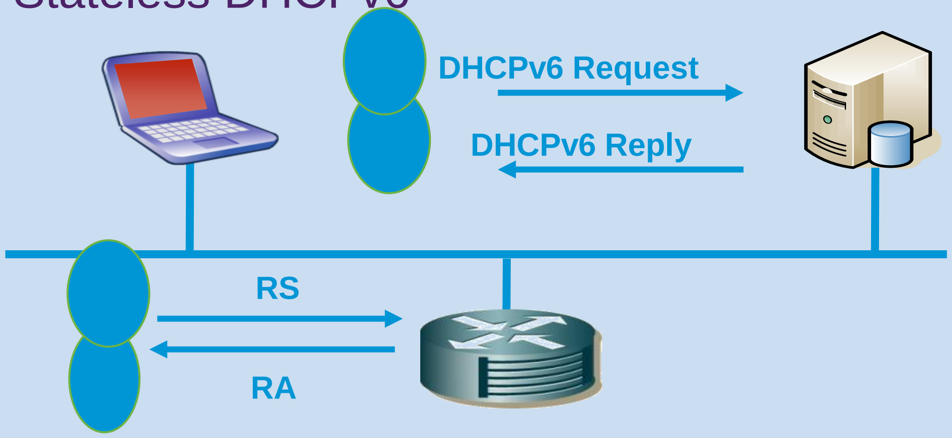
B) Stateless configuration




C) Assigned via Stateful DHCPv6




D) Stateless DHCPv6




E) DHCPv6 Prefix Delegation (PD)

© 2010 Cisco and/or its affiliates. All rights reserved.

# Router configuration for setting flags

- M-bit

  By default the M-bit is not set. To set it:

```
interface FastEthernet0/0
  ipv6 nd managed-config-flag
```

- O-bit

  By default, the O-bit is not set, To set it:

```
interface FastEthernet0/0
  ipv6 nd other-config-flag
```

- A-bit

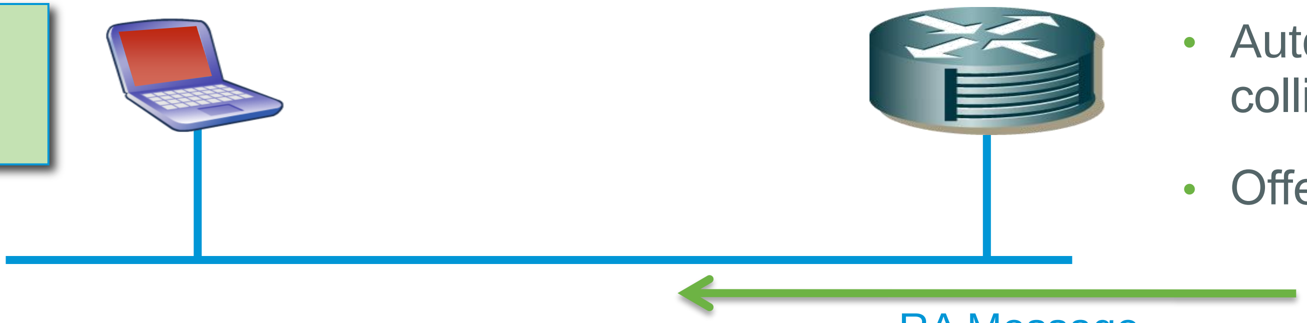
  By default the A bit is set. To disable it:

```
interface FastEthernet0/0
  ipv6 nd prefix 2001:12::/64 300 300 no-autoconfig
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# 1 – Address Autoconfiguration (SLAAC)

Subnet Prefix +
Interface-ID



- Autoconfiguration with "no collisions"
- Offers "plug and play"

At boot time, an IPv6 host build a Link-Local address, then its global IPv6 address(es) from RA

RA Message
Sends Network-Type Information

1. Router Advertisement (RA) sent with "A-Flag" = ON
(Default behavior)

## Default Configuration

```
ipv6 unicast-routing
interface Vlan101
 ip address 10.101.101.254 255.255.255.0
 ipv6 address 2001:DB8:1:CAFE::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1:CAFE::/64 300 300
```

A-Flag set to ON by default
M-Flag set to OFF by default

Indicates that the host should use auto-configuration for address assignment

© 2010 Cisco and/or its affiliates. All rights reserved.

RFC2462

# 1 - Using Autoconfiguration

```
C:\> netsh int ipv6 sh addr
<snip>
Interface 11: Local Area Connection

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Temporary  Preferred        4m26s      4m26s 2001:db8:1:cafe:a588:46c6:6024:33a5
Public     Preferred        4m26s      4m26s 2001:db8:1:cafe:b407:e685:fb14:c12d
Other      Preferred     infinite   infinite fe80::b407:e685:fb14:c12d%11

C:\>
```

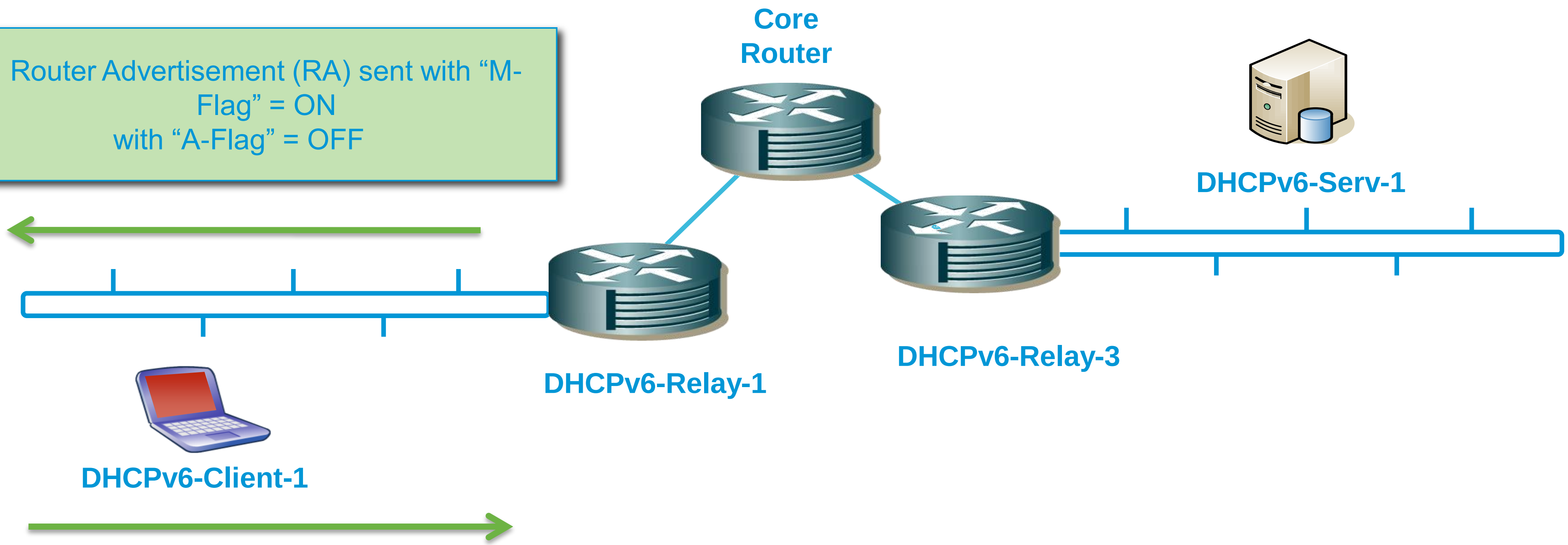
- Windows 7 doesn’t use the EUI-64 technique by default when forming its interface identifier.
- Randomized address are generated for non-Temporary autoconfigured addresses including public and link-local – used instead of EUI-64 addresses
- Win7 host gets 2 global addresses – using SLAAC (Public and Temporary)

© 2010 Cisco and/or its affiliates. All rights reserved.

# 2 – Stateful DHCP only

## RAs Can Be Used to Control DHCPv6 Client Behavior

1. Router Advertisement (RA) sent with "M-Flag" = ON
with "A-Flag" = OFF




2. Client sends DHCPv6 SOLICIT

© 2010 Cisco and/or its affiliates. All rights reserved.

# 2a – Using only the M-Flag

## Using Stateful DHCP – Configuration Sample

```
ipv6 dhcp pool DATA-IPv6
 address prefix 2001:DB8:1:CAFE::/64 lifetime 600 600
 domain-name rack-campus.cisco.com
interface Vlan101
 ip address 10.101.101.254 255.255.255.0
 ipv6 address 2001:DB8:1:CAFE::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1:CAFE::/64 300 300
 ipv6 nd managed-config-flag
 ipv6 dhcp server DATA-IPv6
```

Specifies an address prefix for address assignment.

Set the M-flag. Indicates that the host should use DHCP for stateful address assignment

Specifies the IPv6 Pool name.

```
SW1#sh ipv6 dhcp binding
Client: FE80::B407:E685:FB14:C12D (Vlan101)
  DUID: 000100011 2DFBC30000C29616F1F
  IA NA: IA ID 0x0E000C29, T1 300, T2 480
    Address: 2001:DB8:1:CAFE:5882:DEA4:A3C:570C
            preferred lifetime 600, valid lifetime 600
            expires at Apr 19 1993 09:50 PM (587 seconds)
SW1#
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# 2a – Using only the M-Flag

## Results: Win7 host gets 3 Global Addresses

```
C:\> netsh int ipv6 sh addr
<snip>
Interface 11: Local Area Connection

Addr Type  DAD State    Valid Life Pref. Life Address
---------  ------------ ---------- ---------- -------------------------
Dhcp       Preferred         9m28s      9m28s 2001:db8:1:cafe:5882:dea4:a3c:570c
Temporary  Preferred         4m26s      4m26s 2001:db8:1:cafe:a588:46c6:6024:33a5
Public     Preferred         4m26s      4m26s 2001:db8:1:cafe:b407:e685:fb14:c12d
Other      Preferred      infinite   infinite fe80::b407:e685:fb14:c12d%11

C:\>
```

- Win7 host gets 3 global addresses – one using DHCP, two using SLAAC (Public and Temporary)
- Both SLAAC and DHCP runs independently, and this is the default behavior when only setting the M-Flag
- To only have DHCP, the A-Flag has to be cleared (see next slide)

© 2010 Cisco and/or its affiliates. All rights reserved.

# 2b – Using Stateful DHCP and disabling SLAAC

```
ipv6 unicast-routing
!
ipv6 dhcp pool DATA-IPv6
 address prefix 2001:DB8:1:CAFE::/64 lifetime 600 600
 domain-name rack-campus.cisco.com
!
interface Vlan101
 ip address 10.101.101.254 255.255.255.0
 ipv6 address 2001:DB8:1:CAFE::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1:CAFE::/64 300 300 no-autoconfig
 ipv6 nd managed-config-flag
 ipv6 dhcp server DATA-IPv6
```

Set the A-Flag (autoconfig bit) to OFF.
Indicates that the host should not use SLAAC.

Set the M-Flag (Managed address configuration bit) to ON.
Indicates that the host should use DHCP for stateful address assignment

© 2010 Cisco and/or its affiliates. All rights reserved.

# 2b – Using Stateful DHCP and disabling SLAAC

```
SW1#sh ipv6 dhcp binding
Client: FE80::B407:E685:FB14:C12D (Vlan101)
  DUID: 0001000112DFBC30000C29616F1F
  IA NA: IA ID 0x0E000C29, T1 300, T2 480
    Address: 2001:DB8:1:CAFE:A826:E48D:9153:3B23
            preferred lifetime 600, valid lifetime 600
            expires at Apr 19 1993 09:55 PM (512 seconds)
```

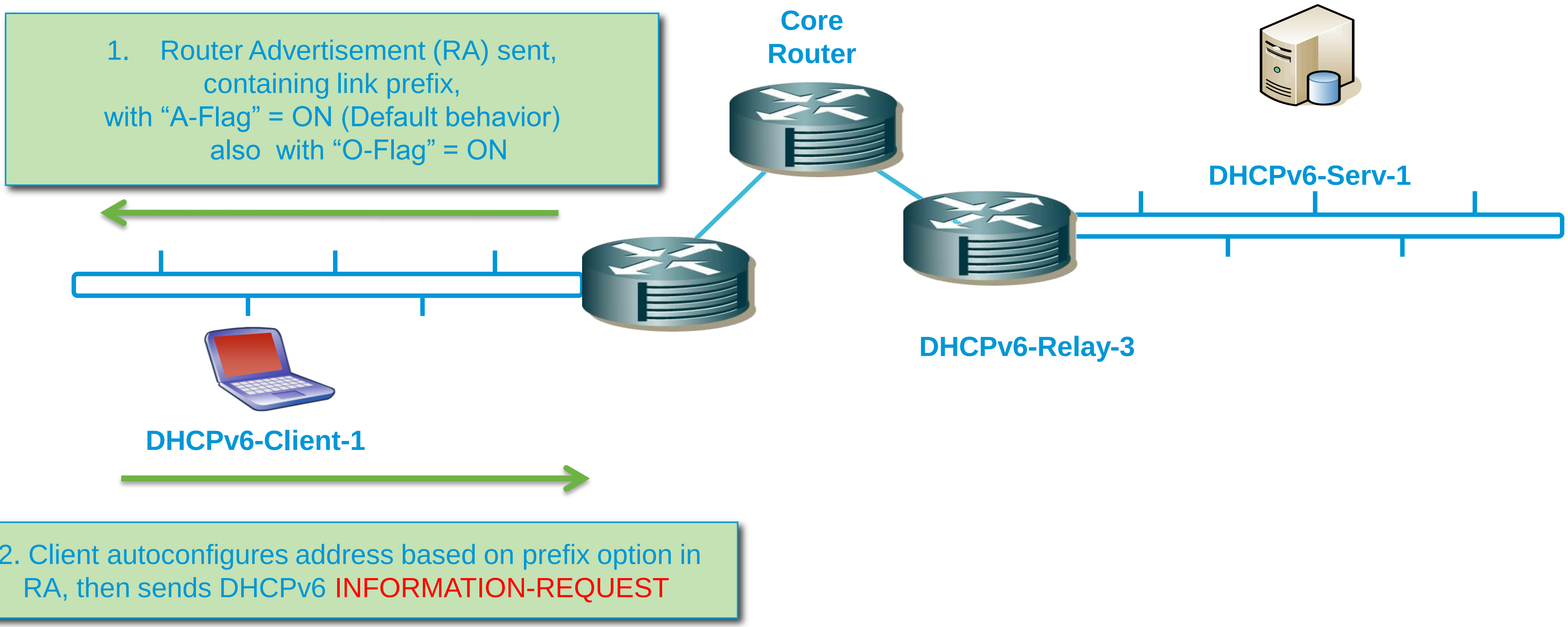
```
C:\> netsh int ipv6 sh addr
<snip>
Interface 11: Local Area Connection

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Dhcp       Preferred        9m47s      9m47s 2001:db8:1:cafe:a826:e48d:9153:3b23
Other      Preferred     infinite   infinite fe80::b407:e685:fb14:c12d:11
```

- Win7 host has only one global address using DHCP

© 2010 Cisco and/or its affiliates. All rights reserved.

# 3 – Stateless DHCP

Stateless DHCPv6 normally combines stateless auto-configuration for address assignment, DHCPv6 exchange for all other configuration settings




© 2010 Cisco and/or its affiliates. All rights reserved.

# 3 – Using Stateless DHCP
## Configuration Sample

```
ipv6 unicast-routing
!
ipv6 dhcp pool DATA-IPv6
 domain-name rack-campus.cisco.com
 dns-server 2001:DB8:1:CAFE::2
 information refresh 1
!
interface Vlan101
 ip address 10.101.101.254 255.255.255.0
 ipv6 address 2001:DB8:1:CAFE::1/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1:CAFE::/64 300 300
 ipv6 nd other-config-flag
 ipv6 dhcp server DATA-IPv6
```

There is no need for an address prefix for address assignment.

Defines how often clients should refresh the config

Set the O-Flag (Other configuration bit) Indicates that the host should use DHCP for stateless address assignment

Specifies the IPv6 Pool name.

© 2010 Cisco and/or its affiliates. All rights reserved.

# Components of DHCPv6

- Remember that there are 4 components in a DHCPv6 setup
  - Servers
  - Clients
  - Relays
  - Routers
- These components can be separate devices or can reside on the same device
  - For e.g. A router running IOS can be configured to be one or more of the following - a DHCPv6 server, a DHCPv6 client on a certain interface, just a router sending ND messages on a IPv6 enabled interface or a relay agent
- When dealing with a router, always remember what function it serves in a DHCPv6 setup. This will help your troubleshooting
- End hosts usually serve as clients only (Windows, macos, Linux etc)

© 2010 Cisco and/or its affiliates. All rights reserved.

# DHCPv6 – IOS

© 2010 Cisco and/or its affiliates. All rights reserved.

# IOS – DHCPv6 Server

- Earlier IOS versions supported only stateless DHCPv6
- Features supported
  - DHCPv6 Prefix Delegation
  - DHCP for IPv6 Relay Agent
  - DHCPv6 Client Information Refresh Option
  - DHCPv6 Server Stateless Auto Configuration
  - Statelful DHCPv6
- **Memory + resource limitations/scalability**
  - **Dual stack hosts impacted more**
- DHCP binding database by default is stored in memory and can optionally be stored on local or remote storage (e.g. FTP, TFTP or RCP) in case of device failure

© 2010 Cisco and/or its affiliates. All rights reserved.

# IOS Configuration – DHCPv6 Server

- Sample Stateful DHCPv6 Server Configuration

```
ipv6 dhcp pool DHVPv6-POOL
 address prefix 2001:DB8:1:CAFE::/64 lifetime 3600 1800
 dns-server 2001:DB8:1:CAFE::84
 domain-name cisco.com
interface GigbitEthernet0/0
 ipv6 dhcp pool DHVPv6-POOL
```

- To configure a stateless DHCPv6 server, just create a pool without the ‘address prefix’ command

- show commands

```
Router#show ipv6 dhcp pool
DHCPv6 pool: DHVPv6-POOL
  Address allocation prefix: 2001:DB8:1:CAFE::/64 valid 3600 preferred 1800 (0 in use, 0 conflicts)
  DNS server: 2001:DB8:1:CAFE::84
  Domain name: cisco.com
  Active clients: 0
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# IOS Configuration – DHCPv6 Server

- show commands
  - show ipv6 dhcp pool
  - show ipv6 dhcp binding
  - show ipv6 dhcp database
- debug commands
  - debug ipv6 dhcp detail
  - debug ipv6 dhcp database

© 2010 Cisco and/or its affiliates. All rights reserved.

# IOS Configuration – DHCPv6 Relay

- A router running IOS can be configured to a DHCP relay using the following command

```
interface Gi0/0
 ipv6 dhcp relay destination 2001:DB8:1:CAFE::84
```

connecting to the server

- show commands

```
Router#show ipv6 dhcp interface
GigabitEthernet0/0 is in relay mode
  Relay destinations:
  2001:DB8:1:CAFE::84
```

- debug commands

```
debug ipv6 dhcp relay
debug ipv6 dhcp detail
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# IOS Configuration – DHCPv6 Client

- An interface in IOS can obtain the IPv6 address in 2 ways
- Autoconfiguration
    - If the RA messages received have the O-bit set, stateless DHCPv6 is used
    - M-bit is ignored by the IOS client

```
interface Gi0/0
 ipv6 address autoconfig
```

- DHCPv6
    - Newer IOS versions (12.4(24)T and later) allow IOS to be a DHCPv6 client
    - All bits (M,O,A) are ignored and stateful DHCPv6 is performed

```
interface Gi0/0
 ipv6 enable
 ipv6 address dhcp [rapid-commit]
 ipv6 nd autoconfig prefix
```

Remember ‘ipv6 enable’ is required as DHCPv6 operates at Layer 3 only and a valid IPv6 source address is required to send DHCPv6 packets

© 2010 Cisco and/or its affiliates. All rights reserved.

# IOS Configuration – DHCPv6 Client cont.

```
interface Gi0/0
 ipv6 enable
 ipv6 address autoconfig
 ipv6 address dhcp [rapid-commit]
 ipv6 nd autoconfig prefix
```

- If both autoconfig and dhcp are configured the client will do both SLAAC and DHCPv6
  - stateless if M-bit unset and O-bit set
  - stateful if M-bit set (O-bit is ignored)

© 2010 Cisco and/or its affiliates. All rights reserved.

# IOS Configuration – DHCPv6 Client

- Be careful when using ‘ipv6 address dhcp’ command
- Unlike DHCP, where subnet mask is provided in DHCP options, DHCPv6 does not provide a prefix length
  - Hosts are supposed to get prefix length from the RA messages sent by the router on the link
- But IOS behaves differently. Therefore, when the IOS DHCPv6 client gets a IPv6 address, it uses a 128-bit mask
- This is a problem – The IPv6 routing table shows a host route for the prefix, so the router will not be able to communicate with other hosts in the same prefix
- Solution – See CSCsm40005
  - Configure ‘ipv6 nd autoconfig prefix’. This will install a route for the prefix advertised by the router on the link.

© 2010 Cisco and/or its affiliates. All rights reserved.

# DHCPv6 – Cisco Network Registrar

© 2010 Cisco and/or its affiliates. All rights reserved.

# Cisco Network Registrar (CNR) and DHCPv6

| DHCPv6 Feature | 6.2/6.3 | 7.0 | 7.1 | 7.2 | 7.3 or 8.0 |
|---|---|---|---|---|---|
| Basic DHCPv6 (address and prefix delegation) | | | | | |
| Client Classing (expressions) | | | | | |
| Reservations (static only) | | | | | |
| DNS Updates (over IPv4) | | | | | |
| LDAP (lookup only, no writes) | | | | | |
| Extensions (DEX & TCL) | | | | | |
| Prefix Utilization Counters (current only) | | | | | |
| Lease History | | | Saved | | |
| Limitation IDs | | | | | |
| Failover / Redundancy | | | | | Planned |
| DHCPv6 Client Reconfiguration (and RKAP) | | | | | |
| DHCPv6 Authentication (beyond RKAP) | | | | | |
| Dynamic Prefix Management (no reload) | | | | | |
| Prefix/link-templates (management) | | | | | |
| DHCPv6 LeaseQuery (RFC 5007) | | | | | |
| DHCPv6 Bulk Leasequery (RFC 5460) | | | | | |

© 2010 Cisco and/or its affiliates. All rights reserved.

# CNR DHCPv6 Configuration

- Mostly identical to how DHCPv4 is configured
- Except Links and Prefixes configured instead of Scopes
  - A Link represents a “physical” network segment
  - A Prefix specifies address or prefix delegation space and can specify a Link name
  - Address assignment/prefix delegation can occur from all Prefixes on a Link.
- Policies extended with additional DHCPv6 attributes and options
  - Rapid Commit, Reconfigure, Temporary addresses, Lifetimes, …

© 2010 Cisco and/or its affiliates. All rights reserved.

# CNR Configuration Steps

- Create Links (optional) and Prefixes
  - May need links to tie multiple prefixes together such as to match incoming traffic's source or if using selection tags
- Create/edit policies, such as default policy, for DHCPv6-specific attributes and set them on Links or Prefixes
  - Use Web UI and see "DHCPv6 Settings" grouping
  - Some other attributes apply to DHCPv6 as well
- Configure IPv6 interfaces for the DHCP server (optional)
  - Only needed if IPv4 interfaces were explicitly configured or not all interfaces can be used (note that you may have to configure IPv4 interfaces as well in the latter case)
- Reload the server!
  - Required for all DHCPv6 related configuration changes!
- Send in packets

For details refer to the CNR User Guide – Managing DHCPv6

© 2010 Cisco and/or its affiliates. All rights reserved.

# CNR Configuration Example – DHCPv6

- Prefixes and Links

```
# Create a link
nrcmd> link example-link create [<attribute=value>]

# Create a prefix
# use attribute "dhcp-type=stateless" for stateless
nrcmd> prefix example-prefix create 2001:0db8::/32 [<attribute=value>]

# Reload the dhcp service
nrcmd> dhcp reload
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# Further Exploration

- We just touched upon the basics of DHCPv6
- There is so much to DHCPv6 that we can have a complete bootcamp based on it
- To explore further, refer to,
  - RFC 3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
  - RFC 3633 - IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
  - RFC 3736 - Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
- IETF Dynamic Host Configuration Working Group
  - https://datatracker.ietf.org/wg/dhc/charter/

© 2010 Cisco and/or its affiliates. All rights reserved.

# Other Management Protocols

© 2010 Cisco and/or its affiliates. All rights reserved.

# Other Management Protocols

- Most other Management Protocols in IOS do support IPv6 at some level, although support may vary
- Following are some of the protocols that support IPv6
  - Netflow v9
  - SSH and telnet – Client and Server
  - ping and traceroute
  - Syslog, HTTP/HTTPS Client and Server
- Management Instrumentations in IOS have some level of IPv6 support
  - EEM, Tcl, Netconf, CNS Agents, etc.
- For up-to-date information on these protocols, it is best to refer to the IPv6 Configuration Guide chapter on Network Management for the particular IOS version you are interested in

© 2010 Cisco and/or its affiliates. All rights reserved.

# Cisco Discovery Protocol - CDP

- IPv6 enhancements allow CDP to exchange IPv6 and neighbor addressing information

```
Router#show cdp neighbors gigabitEthernet 0/0 detail
-------------------------
Device ID: NMS-BB-SW-ROW-13-19
Entry address(es):
  IP address: 172.16.174.251
  IPv6 address: FE80::219:E8FF:FE95:8BC0  (link-local)
Platform: cisco WS-C2960G-48TC-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/0,  Port ID (outgoing port): GigabitEthernet0/2
Holdtime : 166 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Thu 02-Dec-10 08:16 by prod_rel_team
```

- The CISCO-CDP-MIB is IPv6 aware, but support is still not available in IOS - CSCuk33150

© 2010 Cisco and/or its affiliates. All rights reserved.

# Management Protocols Examples

- Example of an IPv6 ping

```
NMS-2911-A#ping 2001:12::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:12::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/8 ms
```

- Example of the copy command using IPv6

```
Router# copy running-config tftp://[2001:12::1]/running-config
```

In Cisco IOS Release 12.2(8)T or later releases, a literal IPv6 address specified with a port number must be enclosed in square brackets ([ ]) when the address is used in source or destination URLs; a literal IPv6 address specified without a port number need not be enclosed in square brackets. Refer to RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, for more information on the use of square brackets with literal IPv6 address in URLs.

© 2010 Cisco and/or its affiliates. All rights reserved.

# Management Protocols Examples

- The 'ip http server' command does not allow an IPv6 ACL

  To prevent http access over IPv6, disable the http server

```
no ip http server
no ip http secure-server
```

- Syslog messages can be sent to IPv6 destinations

```
logging host ipv6 2001::12:1
```

- telnet and SSH access can be restricted using IPv6 ACLs

```
line vty 5 15
 access-class IPv6-NMS in
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# Management Instrumentation Examples

- EEM 3.0 supports IPv6 for,
  - Sending Emails – SMTP Server
  - SNMP Notification source and destination address

```
event manager applet NMS-TEST
action 1.0 mail server "2001:12::1" to "null@cisco.com" from "router@cisco.com" subject
"Hello IPv6”
```

- CNS Agents support IPv6

```
cns config initial 2001:12::1
```

© 2010 Cisco and/or its affiliates. All rights reserved.

# Key Takeaways

- IPv6 support is available in some areas of Network Management
- Additional support is being worked upon and is being added every day
- The Feature Information section of the Network Management Chapter in the IPv6 Configuration Guide is a good place to look for exact IOS version which introduced support for IPv6 for a particular feature
  - IOS 15.1 NMS Feature Support
- Keep a watch for bugs as basic functionality may be broken

© 2010 Cisco and/or its affiliates. All rights reserved.

Thank you.