Global Knowledge

# Bridging and Switching

© 2004 Global Knowledge - All rights reserved

Global Knowledge

## Bridging and Switching

- Frame relay
- Catalyst configuration: VLANs, VTP, STP, MSTP, RSTP, Trunk, Etherchannel, management, features, advanced configuration, Layer 3

© 2004 Global Knowledge - All rights reserved

# IP IGP Routing

© 2004 Global Knowledge - All rights reserved

Global Knowledge

# IP IGP Routing

- OSPF
- EIGRP
- RIPv2
- IPv6: Addressing, RIPng, OSPFv3
- GRE
- ODR
- Filtering, redistribution, summarization and other advanced features

© 2004 Global Knowledge - All rights reserved

Global Knowledge

# BGP

© 2004 Global Knowledge - All rights reserved

Global Knowledge

# BGP

- IBGP
- EBGP
- Filtering, redistribution, summarization, synchronization, attributes and other advanced features

© 2004 Global Knowledge - All rights reserved

Global Knowledge
IP and IOS Features
© 2004 Global Knowledge - All rights reserved

Global Knowledge

# IP and IOS Features

- IP addressing
- DHCP
- HSRP
- IP services
- IOS user interfaces
- System management
- NAT
- NTP
- SNMP
- RMON
- Accounting

© 2004 Global Knowledge - All rights reserved

Global Knowledge

# IP services

- TCP
  - TCP Performance Parameters
  - TCP Window Scaling
  - TCP Explicit Congestion Notification
- Server Load Balancing
- Web Cache Services
- First Hop Redundancy
  - HSRP
  - VRRP
  - GLBP
- Next Hop Resolution Protocol

© 2004 Global Knowledge - All rights reserved

## TCP Performance Parameters

1. Router(config)# **ip tcp synwait-time** *seconds*
2. Router(config)# **ip tcp path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}]
3. Router(config)# **ip tcp selective-ack**
4. Router(config)# **ip tcp timestamp**
5. Router(config)# **ip tcp chunk-size** *characters*
6. Router(config)# **ip tcp window-size** *bytes*
7. Router(config)# **ip tcp queuemax** *packets*

© 2004 Global Knowledge - All rights reserved

1. Sets the amount of time the Cisco IOS software will wait to attempt to establish a TCP connection.The default is 30 seconds.
2. Enables Path MTU Discovery.
3. The TCP selective acknowledgment feature improves performance in the event that multiple packets are lost from one TCP window of data.
4. The TCP time-stamp option provides better TCP round-trip time measurements.
5. By default, for Telnet and rlogin, the maximum number of characters that TCP reads from the input queue at once is a very large number (the largest possible 32-bit positive number).
6. The default TCP window size is 2144 bytes.
7. The default TCP outgoing queue size per connection is 5 segments if the connection has a TTY associated with it (like a Telnet connection). If no TTY connection is associated with it, the default queue size is 20 segments.

Global Knowledge

## TCP

1. Router(config)# **ip tcp window-size** *bytes*
2. Router(config)# ip tcp ecn

© 2004 Global Knowledge - All rights reserved

1. Specifies the scaled TCP window size. The *bytes* argument can be set to an integer from 0 to 1,073,741,823. To enable window scaling to support LFNs, the TCP window size must be more than 65,535. The default window size is 4128 if window scaling is not configured.
2. The TCP Explicit Congestion Notification (ECN) feature provides a method for an intermediate router to notify the end hosts of impending network congestion. It also provides enhanced support for TCP sessions associated with applications that are sensitive to delay or packet loss including Telnet, web browsing, and transfer of audio and video data. The benefit of this feature is the reduction of delay and packet loss in data transmissions.

## Server Load Balancing

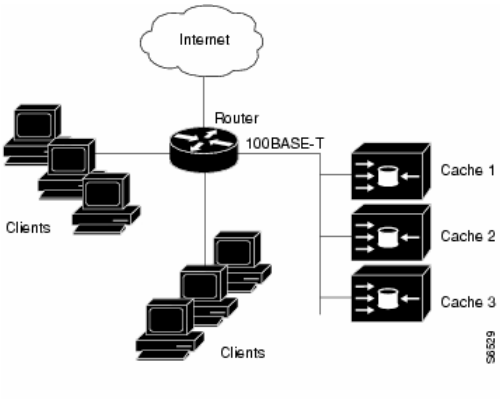
```
ip slb serverfarm PUBLIC
  predictor leastconns
  real 10.1.1.1
    weight 16
    inservice
  real 10.1.1.2
      weight 4
      maxconns 1000
      inservice
  real 10.1.1.3
      weight 24
      inservice
ip slb vservers PUBLIC_HTTP
  virtual 10.0.0.1 tcp www
  serverfarm PUBLIC
  inservice
```

© 2004 Global Knowledge - All rights reserved

The SLB feature is a Cisco IOS-based solution that provides IP server load balancing. Using the IOS SLB feature, the network administrator defines a *virtual* server that represents a group of *real* servers in a cluster of network servers known as a *server farm*. In this environment the clients are configured to connect to the IP address of the virtual server. The virtual server IP address is configured as a loopback address, or secondary IP address, on each of the real servers. When a client initiates a connection to the virtual server, the IOS SLB function chooses a real server for the connection based on a configured load-balancing algorithm.

Global Knowledge

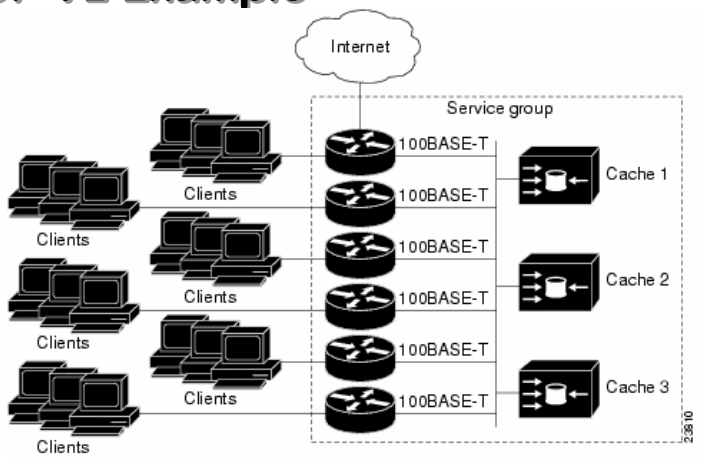
# WCCP V1 Example




© 2004 Global Knowledge - All rights reserved

Global Knowledge

# WCCP V2 Example




© 2004 Global Knowledge - All rights reserved

Global Knowledge

## Web Cache Services

```
Router# ip wccp version {1 | 2}
```

- The following example shows a general WCCPv2 configuration session:

```
Router(config)# ip wccp web-cache group-address 224.1.1.100
   password alaska1
```

- The following example shows a web cache service configuration session:

```
router(config)# ip wccp web-cache
router(config)# interface ethernet 0
router(config-if)# ip wccp web-cache redirect out
```

- The following assumes you a configuring a service group using Cisco Cache Engines, which use dynamic service 99 to run a reverse proxy service:

```
router(config)# ip wccp 99
router(config)# interface ethernet 0
router(config-if)# ip wccp 99 redirect out
```

© 2004 Global Knowledge - All rights reserved

The Web Cache Communication Protocol (WCCP) is a Cisco-developed content-routing technology that allows you to integrate cache engines (such as the Cisco Cache Engine 550) into the network infrastructure. Cisco IOS Release 12.1 and later releases allow the use of either Version 1 (WCCPv1) or Version 2 (WCCPv2) of the WCCP. The Cisco IOS WCCP feature allows utilization of Cisco Cache Engines (or other caches running WCCP) to localize web traffic patterns in the network, enabling content requests to be fulfilled locally. Traffic localization reduces transmission costs and download time. With WCCP-Version 1, only a single router services a cluster. Multiple routers can use WCCPv2 to service a cache cluster. The caching engines need to point to the control router(s) using a either their unicast IP address or you can use a multicast address to identify the group of routers.  There is an optional password that can be added.

# Hot Standby Router Protocol

- **Router 1**

```
key chain hsrp1
 key 0
  key-string 54321098452103ab


interface Ethernet0/1
 standby 1 authentication md5 key-chain hsrp1
 standby 1 ip 10.21.0.10
 standby 1 preempt delay minimum 20
```

- **Router 2**

```
interface Ethernet0/1
 standby 1 authentication md5 key-string
  54321098452103ab
 standby 1 ip 10.21.0.10
```

© 2004 Global Knowledge - All rights reserved

# Virtual Router Redundancy Protocol

**Router 1**

```
track 1 interface Serial0/1 line-protocol
!
interface Ethernet1/0
 ip address 10.0.0.1 255.0.0.0
 vrrp 1 ip 10.0.0.3
 vrrp 1 priority 120
 vrrp 1 track 1 decrement 15
```

**Router 2**

```
interface Ethernet1/0
 ip address 10.0.0.2 255.0.0.0
 vrrp 1 ip 10.0.0.3
```

© 2004 Global Knowledge - All rights reserved

## Gateway Load Balancing Protocol

```
track 1 interface POS 5/0 ip routing
track 2 interface POS 6/0 ip routing
interface fastethernet 0/0
 glpb 10 weighting 110 lower 95 upper 105
 glbp 10 weighting track 1 decrement 10
 glbp 10 weighting track 2 decrement 10
 glbp 10 forwarder preempt delay minimum 60
```

**Default preempt delay is 30 seconds**
**Default weight is 100, with a lower of 1 and upper of 100.**

© 2004 Global Knowledge - All rights reserved

The Gateway Load Balancing Protocol feature provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first hop routers on the LAN combine to offer a single virtual first hop IP router while sharing the IP packet forwarding load. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.

Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The function of the AVG is that it assigns a virtual MAC address to each member of the GLBP group. The AVG is also responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address from clients (PCs).

Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address.

## NAT – Stateful NAT with HSRP

**The following example shows how to configure SNAT with HSRP:**

```
!
Int fa 0/0
 standby name SNATHSRP
 standby ip 10.1.1.1
 standby delay reload 60
 standby preempt delay minimum 60 reload 60 sync 60
!
ip nat Stateful id 1
 redundancy SNATHSRP
  mapping-id 10
  protocol udp
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id
   10 overload
ip classless
ip route 10.1.1.0 255.255.255.0 Null0
```

© 2004 Global Knowledge - All rights reserved

This command has two forms: HSRP stateful NAT and manual stateful NAT. The form that uses the keyword **redundancy** establishes the HSRP redundancy method. When HSRP mode is set, the primary and backup NAT routers are elected according to the HSRP standby state. To enable stateful NAT manually, configure the primary router and backup router.

In HSRP mode, the default TCP can be changed to UDP by using the optional **protocol udp** keywords with the **redundancy** keyword.

# NAT – Stateful NAT Manual

**On both routers:**

```
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1
   mapping-id 10 overload
ip route 10.1.1.0 255.255.255.0 Null0
```

**On Router A:**

```
ip nat stateful id 1
 primary 10.88.194.17
  peer 10.88.194.18
  mapping-id 10
```

**On Router B:**

```
ip nat stateful id 2
 backup 10.88.194.18
  peer 10.88.194.17
  mapping-id 10
```

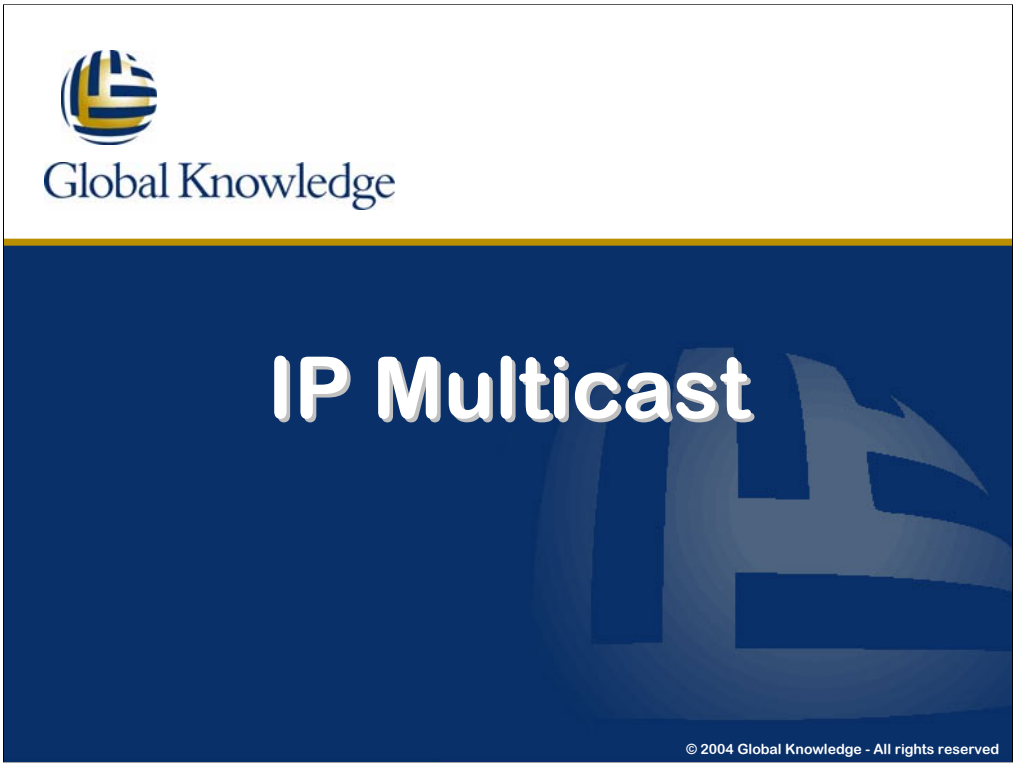
© 2004 Global Knowledge - All rights reserved

## NAT Protocol Translation

```
Interface fa 0/0
 ip address 180.40.7.7 255.255.255.0
 ipv6 nat
!
Interface s 1/0
 ipv6 address 2005:0:307::7/64
 ipv ospf 1 area 0
 ipv6 nat
!
router rip
 version 2
 redistribute static metric 2
 network 180.40.0.0
 no auto-summary
!
ip route 33.33.33.0 255.255.255.0 Null0
!
ipv6 router ospf 1
 router-id 7.7.7.7
 log-adjacency-changes
 distribute-list prefix-list ProbE out connected
 redistribute connected
!
ipv6 nat v4v6 source list 1 pool ProbE
ipv6 nat v4v6 pool ProbE 2006:6:6::1 2006:6:6::F prefix-length 96
ipv6 nat v6v4 source 2005:0:237:0:212:7FFF:FE7D:3A00 33.33.33.33
ipv6 nat prefix 2006:6:6::/96
ipv6 prefix-list ProbE seq 5 permit 2006:6:6::/96
```

© 2004 Global Knowledge - All rights reserved

You must identify the interfaces involved using the ipv6 nat command, note that there is no direction. You have to determine if you want to have a dynamic pool for IPv4 or IPv6, you can't have dynamic nat for both, one must be a static configuration. In this example, there is a static translation for an IPv6 address to a IPv4 address. There rest is to support a dynamic pool for IPv4 to IPv6. You have to identify a prefix that is going to be used for the nat process, note that it has to be a /96 even though the help shows a range of 0-128. The prefix will show up in the IPv6 RIB as a connected route. To get the IPv6 prefix advertised to the other IPv6 routers, redistribute connected into which ever routing protocol you are using. For the IPv4 prefix, you'll need to either add an address to a loopback interface or create a static route to null 0. Then pass that into the routing protocol for IPv4. The concept for the pools is standard nat.


Global Knowledge
IP Multicast
© 2004 Global Knowledge - All rights reserved

Global Knowledge

# IP Multicast

- PIM, bi-directional PIM
- MSDP
- Multicast tools, source specific multicast
- DVMRP
- Anycast

© 2004 Global Knowledge - All rights reserved

Global Knowledge

# QoS

© 2004 Global Knowledge - All rights reserved

Global Knowledge

## QoS

- Quality of service solutions
- Classification
- Congestion management, congestion avoidance
- Policing and shaping
- Signaling
- Link efficiency mechanisms
- Modular QoS command line

© 2004 Global Knowledge - All rights reserved

# 3550 MLS QoS Maps

```
Dscp-cos map:
    d1 :  d2 0  1  2  3  4  5  6  7  8  9
    ------------------------------------
--
     0 :    00 00 00 00 00 00 00 00 01 01
     1 :    01 01 01 01 01 01 02 02 02 02
     2 :    02 02 02 02 03 03 03 03 03 03
     3 :    03 03 04 04 04 04 04 04 04 04
     4 :    05 05 05 05 05 05 05 05 06 06
     5 :    06 06 06 06 06 06 07 07 07 07
     6 :    07 07 07 07

Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
    -------------------------------
      dscp:   0  8 16 24 32 40 48 56
```

```
IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     -------------------------------
       dscp:   0  8 16 24 32 40 48 56

   Dscp-dscp mutation map:
   Default DSCP Mutation Map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
--
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

© 2004 Global Knowledge - All rights reserved

# Configuring PQ on Catalyst 3550 Switches

```
Switch(config)#
wrr-queue cos-map quid cos1...cosn
```

- Assigns CoS values to CoS priority queues
- quid: Specifies the queue ID of the CoS priority queue. (Ranges are 1 to 4 where 1 is the lowest CoS priority queue.)
- cos1...cosn: Specifies the CoS values that are mapped to the queue ID.
- Default ID values are:

| Queue ID | CoS Values |
|---|---|
| 1 | 0, 1 |
| 2 | 2, 3 |
| 3 | 4, 5 |
| 4 | 6, 7 |

© 2004 Global Knowledge - All rights reserved

# Configuring PQ on Catalyst 3560 Switches

```
Switch(config)#
mls qos srr-queue output cos-map quid {cos1...cos8 |
threshold threshold-id cos1...cos8}
Interface gigabitethernet0/1
 queue-set quid
```

- **quid:** Specifies the queue ID of the CoS priority queue. (Ranges are 1 to 4 where 1 is the lowest CoS priority queue.)
- **cos1...cos8:** Specifies the CoS values that are mapped to the queue ID.
- **threshold-id** Map CoS values to a queue threshold ID. For *threshold-id*, the range is 1 to 3. For *cos1...cos8*, enter up to eight values, and separate each value with a space. The range is 0 to 7.

Default ID values are:

| Queue ID | CoS Values | Queue ID | CoS Values |
|---|---|---|---|
| 1 | 5 | 3 | 2, 3 |
| 2 | 0, 1 | 4 | 4, 6, 7 |

© 2004 Global Knowledge - All rights reserved

# Configuring WRR on Catalyst 3550 Switches

```
Switch(config)#
wrr-queue bandwidth weight1...weight4
```

- Assigns WRR weights to the four egress queues
- Ranges for the WRR values:
  - The range is 1 to 255.

```
mls qos
interface FastEthernet0/12
priority-queue out
wrr-queue bandwidth 20 1 80 1
no wrr-queue cos-map
wrr-queue cos-map 1 0 1 2 4
wrr-queue cos-map 3 3 6 7
wrr-queue cos-map 4 5
mls qos map cos-dscp 0 8 16 26 32 46 48 56
!
```

© 2004 Global Knowledge - All rights reserved

# Configuring SRR on Catalyst 3560 Switches

```
Switch(config-if)#
srr-queue bandwidth {shape | share} weight1...weight4
```

- Assigns SRR weights to the four egress queues
- Shape: Specify the weights to specify the percentage of the port that is shaped. The inverse ratio (1/*weight*) specifies the shaping bandwidth for this queue.
- Share: The ratios of *weight1*, *weight2*, *weight3*, and *weight4* specify the ratio of the frequency in which the SRR scheduler dequeues packets (same as WRR).
- Ranges for the SRR values:
  - Shape: The range is 1 to 65535.
  - Share: The range is 1 to 255.

© 2004 Global Knowledge - All rights reserved

# Configuring WRR on Catalyst 3550/3560 Switches – Expedite Queue

```
Switch(config)#
Priority-queue out
```

- Assigns priority queue to queue 4 for the 3550 & queue 1 for the 3560
- Weight is ignored
- Queue 4 is serviced before all other queue
- 1P3Q model


© 2004 Global Knowledge - All rights reserved

# Security

© 2004 Global Knowledge - All rights reserved

Global Knowledge

## Security

- AAA
- Security server protocols
- Traffic filtering and firewalls
- Access lists
- Routing protocols security, catalyst security
- CBAC
- Other security features

© 2004 Global Knowledge - All rights reserved