Cisco™ CCNA ICND2 : Routing Protocols

Routing Protocols

Routing protocols job is to maintain routing tables and route packets appropriately.

Examples of routing are RIP, IGRP, EIGRP, OSPF.

Routed Protocols

Routed protocols are used to transport user traffic from source node to destination node.
Examples of routed protocols are IP, IPX and AppleTalk.

Classful Routing Protocols

Classful routing protocols do not exchange subnet information during routing information exchanges.
The summarization is always done automatically at major network boundaries.
Ex: RIP v1, IGRP

Classless Routing Protocols

In classless routing protocols, subnet information is exchanged during routing updates.
This results in more efficient utilization of IP addresses. The summarization in classless networks is manually controlled. Ex: RIP v2, EIGRP, OSPF, BGP v4, and IS-IS

Types of Routing Protocols

Distance Vector: Distance vector routing determines the direction and distance to any link in the internetwork. Smaller the metric, better the path. Distance vector routing is useful for smaller networks. Ex: RIP and IGRP.

Link State: Also known as SPF algorithms, SPF generates the exact topology of the entire network for route computation by listening to the first hand information. Bandwidth and delay are the most widely used metrics. Ex: OSPF and NLSP.

Balanced Hybrid: Balanced Hybrid combines some aspects of Link State and Distance Vector routing protocols. It uses distance vectors with more accurate metrics to determine the best paths to destination networks. Ex: EIGRP

Default Administrative distances

Directly Connected Interface------> 0
Static Route------> 1
Internal EIGRP------> 90
IGRP------> 100
OSPF------> 110
RIP------> 120
IS-IS------> 115
Unknown 255
External BGP----------> 20
Internal BGP----------> 200
An administrative distance of 0 represents highest trustworthiness of the route.
An administrative distance of 255 represents the lowest trustworthiness of the route.

ARP

Address Resolution Protocol (ARP) is used to resolve a hosts IP address to its physical address (such as MAC address), to allow communication on a multi-access medium such as ethernet.

Reverse ARP (RARP) is used to obtain an IP address from physical address (such as MAC). RARP broadcast may be used to obtain IP address to boot by diskless workstations over a network.

Cisco™ CCNA ICND2 : EIGRP and OSPF

EIGRP (Enhanced Interior Gateway Protocol)

Important terms used in EIGRP

Successor: A route (or routes) selected as the primary route(s) used to transport packets to reach destination. Note that successor entries are kept in the routing table of the router.
Feasible successor: A route (or routes) selected as backup route(s) used to transport packets to reach destination. Note that feasible successor entries are kept in the topology table of a router.
DUAL (Diffusing Update Algorithm): Enhanced IGRP uses DUAL algorithm to calculate the best route to a destination

Routing metrics used by IGRP

Bandwidth: This is represents the maximum throughput of a link.
MTU (Maximum Transmission Unit): This is the maximum message length that is acceptable to all links on the path. The larger MTU means faster transmission of packets.
Reliability: This is a measurement of reliability of a network link. It is assigned by the administrator or can be calculated by using protocol statistics.
Delay: This is affected by the band width and queuing delay.
Load: Load is based among many things, CPU usage, packets processed per sec

For IGRP routing, you need to provide AS (Autonomous System) number in the command. Routers need AS number to exchange routing information. Routers belonging to same AS exchange routing information.

OSPF(Open Shortest Path First)

OSPF and OSPF Area

OSPF is a link state technology that uses Dijkstra algorithm to compute routing information.

An OSPF area is a collection of networks and routers that have the same area identification.OSPF process identifier is locally significant.

OSPF router ID determination

1. Use the address configured by the ospf router-id command
2. Use the highest numbered IP address of a loopback interface
3. Use the highest IP address of any physical interface
4. If no interface exists, set the router-ID to 0.0.0.0

OSPF Priority

The ip ospf priority command is used to set manually which router becomes the DR. The range is 0-255 and the default is 1. 0 means it will never be DR or BDR.

DR and BDR Election

When two or more routers are contending to be a DR (designated Router) on a network segment, the router with the highest OSPF priority will become the DR for that segment. The same process is repeated for the BDR. In case of a tie, the router with the highest RID will win.

OSPF Area Types

Standard Area : Default OSPF area type
Stub Area : External link (type 5) LSAs are replaced with a default route
Totally Stubby Area : Type 3, 4, and 5 LSAs are replaced with a default route
Not So Stubby Area (NSSA) : A stub area containing an ASBR; type 5 LSAs are converted to type 7 within the area

Router Types

Internal Router : All interfaces reside within the same area
Backbone Router : A router with an interface in area 0 (the backbone)
Area Border Router (ABR) : Connects two or more areas
AS Boundary Router (ASBR) : Connects to additional routing domains; typically located in the backbone

Cisco™ CCNA ICND2 : Frame Relay

Types of virtual circuits (Vcs) in Frame Relay

Frame Relay is purely a Layer 2 standard.

Two types of Vcs in FR

1. Permanent Virtual Circuits (PVCs): these are permanently established connections that are used for frequent and consistent data transfers between DTEs across a Frame Relay cloud.

2. Switched Virtual Circuits (SVCs): these are temporary connections used in situations requiring only occasional data transfers between DTEs across Frame Relay cloud. The terms "Call Setup", "Data Transfer", "Idle", and "Call Termination" are associated with SVCs.

Frame relay sub-interfaces

When configuring frame-relay using sub interfaces the physical interfaces on which sub interfaces are configured would not be assigned any IP address. Even if one is assigned it should be removed prior to configuring frame-relay.

If an IP address is assigned to physical interface, the sub interfaces defined within the physical interface will not receive any frames.

Split horizon is a method of preventing a routing loop in a network. To overcome the split horizon, sub-interfaces can be configured on NBMA networks.

Frame Relay connection types

1. Point-to-Point: In point-to-point connection type, a single sub interface establishes a PVC connection to another physical interface or sub-interface

2. Multi-point :In multipoint connection type, a single sub-interface is used to establish multiple PVC connections to several physical interfaces or sub-interfaces. In multipoint Frame-Relay network, split horizon rule is applicable to broadcast traffic.

Frame Relay encapsulation types and LMI Types

Cisco supports two types of Frame Relay encapsulation: **cisco (default), and ietf.** Use IETF when setting up a frame-relay network between a Cisco router and a non-Cisco router.

Frame-Relay LMI types are **Cisco (default), ANSI, Q933A**; LMI type is auto-sensed in IOS v11.2 and up.
Show frame-relay lmi command shows LMI stats.

DLCI (Data Link Connection Identifier)

Salient features

1. DLCIs have only local significance. It means, the end devices over FR network can have different DLCI numbers
2. DLCI number is provided by the FR service provider. DLCI number is mapped to Layer 3 protocol address using 'Frame-Relay map' statement.
3. DLCI numbers must be unique on a router.

DLCI Configuration

The command used to assign dlci number to a sub interface is:
R1(config-if)#frame-relay interface-dlci <dlci-number>
Ex: R1(config-if)#frame-relay interface-dlci 100
Note that prior to issuing the above command; issue the following command to get into proper sub interface configuration mode:
R1(config)#interface serial number.subinterface-number {multipoint | point-to-point} **Ex: R1(config)#interface serial 0.1 point-to-point**

Cisco™ CCNA ICND2 : Access-Lists

Access Lists

IP access lists are a sequential list of permit and deny conditions that apply to IP addresses or upper layer protocols. Access Control Lists are used in routers to identify and control traffic.

Purpose of Access Lists

1. Controlling traffic through a router, and
2. Controlling VTY access to a router's VTY ports
3. Filter incoming and outgoing packets
4. Restrict contents of routing updates
5. Trigger dial-on-demand routing (DDR) calls

Types of IP Access Lists

Standard IP Access Lists
Extended IP Access Lists
Named Access Lists

Wild Card Masking

Wild card masking is used to permit or deny a group of addresses.
For example, if we have a source address 185.54.13.2 and want all the hosts on the last octet to be considered, we use a wild card mask, 185.54.13.255.
The 32 bit wildcard mask consists of 1's and 0's
1 = ignore this bit
0 = check this bit

Special Case: Host 185.54.13.2 is same as 185.54.13.2 with a wild card mask of 0.0.0.0, considers only specified IP.
Any is equivalent to saying 0.0.0.0 with a wild card mask of 255.255.255.255. This means none of the bits really matter. All IP addresses need to be considered for meeting the criteria.

Standard Access List

1. These have the format, **access-list [number] [permit or deny] [source_address]**
Ex: access-list 1 permit 192.168.2.0 0.0.0.255
2. Place standard access lists as near the destination as possible and extended access lists as close to the source as possible.
3. Access lists have an implicit deny at the end of them automatically. Because of this, an access list should have at least one permit statement in it; otherwise the access list will block all remaining traffic.
4. Access lists applied to interfaces default to outbound if no direction is specified.

Extended Access Lists and Named Access Lists

Extended Access lists have the format,
access-list {number}{permit or deny} {protocol} {source}source-wildcard [operator [*port*]]{destination} destination-wildcard [operator [*port*]]
With extended IP access lists, we can act on any of the following:
- Source address
- Destination address
- IP protocol (TCP, ICMP, UDP, etc.)
- Port information (WWW, DNS, FTP, etc.)

Ex: access-list 101 permit icmp host 192.168.3.2 any

Named Access lists have the format, **ip access-list {standard /extended} name**
Ex: ip access-list extended denyping

Permitted numbers for access-lists

1-99: IP standard access list
100-199: IP extended access list
800-899: IPX standard access list
1000-1099: IPX SAP access list
1100-1199: Extended 48-bit MAC address access list
900-999: IPX extended access list

Cisco™ CCNA ICND2 : NAT

Static NAT

Maps an unregistered IP address to registered IP (globally unique) addresses on one-to-one basis.

The command, **ip nat inside source static <local ip> <global ip>** configures address translation for static NAT.

Dynamic NAT

Maps an unregistered IP address to a registered (globally unique) IP address from a group of registered (globally unique) IP addresses.

The command, **ip nat inside source list <access-list-number> pool <name>** is used to map the access-list to the IP NAT pool during the configuration of Dynamic NAT.

Overloading

A special case of dynamic NAT that maps multiple unregistered IP addresses to a single registered (globally unique) IP address by using different port numbers.

Dynamic NAT with overloading is also known also as PAT (Port Address Translation).

Overlapping

This occurs when your internal IP addresses belong to global IP address range that belong to another network.

Defining an IP NAT Pool

1. Defining an IP NAT pool for the inside network using the command:
ip nat pool <pool-name> <start-ip> <end-ip> {netmask <net-mask> | prefix-length <prefix-length>} [type-rotary] ***Ex: ip nat pool pool1 200.200.200.3 200.200.200.4 netmask 255.255.255.0***

Note that type-rotary is optional command. It indicates that the IP address range in the address pool identifies hosts among which TCP load is distributed.

2. Mapping the access-list to the IP NAT pool by using the command:
ip nat inside source list <access-list-number> pool <pool-name> ***Ex: ip nat inside source list 1 pool pool1***

Address Classification

Inside Local : An actual address assigned to an inside host

Inside Global : An inside address seen from the outside

Outside Global : An actual address assigned to an outside host

Outside Local : An outside address seen from the inside

NAT Pool : A pool of IP addresses to be used as inside global or outside local addresses in translations

Configuring NAT

When configuring NAT, NAT should be enabled on at least one inside and one outside interface.

1. The command for enabling NAT on inside interface is:
R1(config-if)#ip nat inside

2. The command for enabling NAT on the outside interface is:

R1(config-if)#ip nat outside

Remember to enter into appropriate configuration modes before entering the commands.

Usually, the inside NAT will be configured on an Ethernet interface, whereas the outside NAT is configured on a serial interface.

Cisco™ CCNA ICND2 : IPv6 Addressing

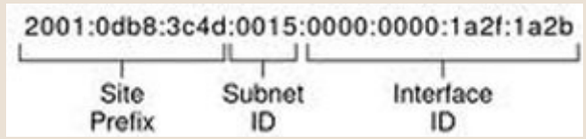
IPv6 : Points to Remember

1. IPv6 address is **128** bits in length represented in hexadecimal
2. IPv6 Loopback address is 0:0:0:0:0:0:0:1, also expressed as **::1**.
3. IPv6 reserves two special addresses. They are **0:0:0:0:0:0:0:0** and **0:0:0:0:0:0:0:1**.
4. Three transition strategies for migration from ipv6 to ipv4 are dual stacking, 6-to-4 tunneling and NAT-PT

IPv6 Addressing

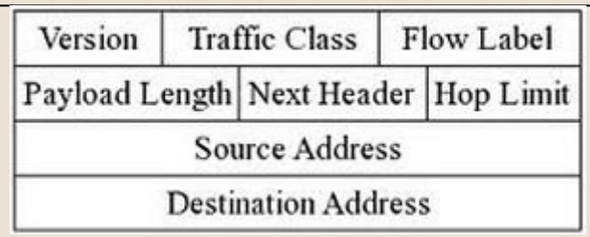
IPv6 address consists of 8 groups of four hexadecimal digits separated by colons and which mainly consists of 3 segments called Global Prefix which is of 48 bits, subnet part with 16 bits and Interface ID called as Host part with 64 bits.

The first 3 octets constitute Global Prefix, the fourth octet constitute subnet part and the last four form the Interface ID.



Rules : a) One set of 0's in the address can be replaced by :: but this can be done only once
b) One or any number of consecutive groups of 0 value can be replaced with two colons (::)

IPv6 Header



Version (4 bits) : IP version number (6)

Traffic Class (8 bits) : Used for QoS

Flow Label (20 bits) : Used for packet labelling

Payload Length (16 bits) : Length of the IPv6 payload

Next Header (8 bits) : Identifies the type of header following the IPv6 header

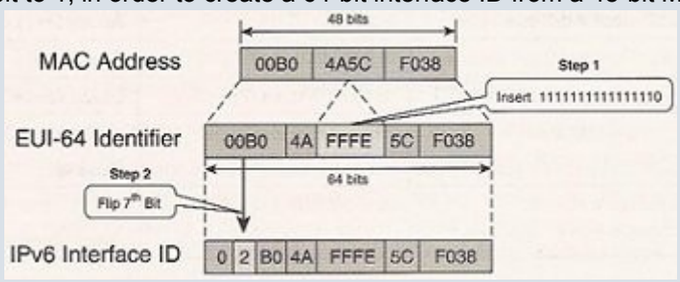
Hop Limit (8 bits) : Number of hops until the packet gets discarded.

Source Address (128 bits) : Source IP address

Destination Address (128 bits) : Destination IP address

EUI-64 Format

MAC to EUI-64 conversion inserts hex “FFFE” in the middle of a MAC addr, Then flips the U/L bit to 1, in order to create a 64-bit interface ID from a 48-bit Mac address.



IPv6 Communication Types

Unicast : used for one-to-one communication. There are 3 types of unicast addresses namely global, unique-local and link-local

Multicast : used for one-to-many communication IPv6 multicast address begins with "FF"

Anycast : used for one-to-one-of-many communication

IPv6 Address Scopes

::/0----------> Default Route
::/128----------> Unspecified
::1/128----------> Loopback
FC00::/7---------> Unique Local Unicast
FE80::/10--------> Link-Local Unicast
FEC0::/10-------> Site-Local Unicast
FF00::/8----------> Multicast

SimulationExams™

YOUR WAY TO CERTIFICATION SUCCESS

Cisco™ CCNA ICND2 : VLANs and VTP

VLANs – Points to Remember

1. VLAN 1 is the management VLAN.
2. **Static VLAN :** VLAN is statically assigned to the physical port and never changes.
3. **Dynamic VLAN :** VMPS automatically assigns VLAN based on MAC
4. **Access Link :** An access link can carry only one VLAN (used between host and switch port)
5. **Trunk Link :** A trunk link can carry multiple VLANs. Used to connect to other switches, routers, or servers
6. Two types of Trunk framing: ISL (Cisco only) and 802.1.q
7. Trunk links can carry 1 to 1005 VLANs
8. Switchport modes are trunk, dynamic desirable, dynamic auto, access.

VTP – Points to Remember

1. VTP is a Layer 2 messaging protocol. It carries configuration information throughout a single domain
2. VTP Modes are
   Server : Create, modify, or delete VLANs (This is the deafult vtp mode on a switch)
   Client : Can't create, change, or delete VLANs
   Transparent : Used when a switch is not required to participate in VTP, but only pass the information to other switches
3. VTP domain is common to all switches participating in VTP
4. Pruning is a technique where in VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic
5. **Configuration revision number** is a 32-bit number that indicates the level of revision for a VTP packet. Each time the VTP device undergoes a VLAN change, the config revision is incremented by one.

VLAN configuration

Creating VLANs

```
SW1#vlan database
SW1(vlan)#vlan 10 name firstvlan
SW1(vlan)#vlan 20 name secondvlan
```

Access Port configuration

```
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#switchport access vlan 20
```

Access port config to a range of interfaces

```
SW1(config)#interface range fa 0/2 - 5
SW1(config-if)#switchport access vlan 10
SW1(config)#interface range fa 0/6 - 10
SW1(config-if)#switchport access vlan 20
```

Trunk Port configuration

```
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk encapsulation dot1q
```

VTP Configuration

```
SW1#vlan database
SW1(vlan)#vtp mode (Server/Client/Transparent)
SW1(vlan)#vtp domain <name>
SW1(vlan)#vtp password <password>
SW1(vlan)#vtp pruning
```

Troubleshooting commands

1. show vlan
2. show vlan-membership
3. show vtp status
4. show interfaces trunk
5. show interface <interface-name> switchport

Cisco™ CCNA ICND2 : Spanning Tree Protocol

STP – Points to Remember

1. STP is a layer 2 protocol that runs on switches and bridges, the purpose of STP is to remove switching loops. By default, STP is enabled on cisco switches.
2. All switches participating in STP exchange info with other switches in the network Through messages known as **BPDUs (**Sent out at a frequency of 2 sec on every port)
3. STP port states are **Blocked, Listen, Learn, Forward, Disabled**
4. The command "show spanning-tree" includes the following info
   i. VLAN number
   ii. Root bridge priority, MAC address
   iii. Bridge timers (Max Age, Hello Time, Forward Delay)

STP Port Roles

1. **Root** : A bridge can have only one root port. The root port is the port that leads to the root bridge. All bridges except the root bridge will have a root port. the root port is in the STP forwarding state.
2. **Designated** : One designated port is elected per link (segment). The designated port is the port closest to the root bridge. Each designated port is in the STP forwarding state
3. **Alternate** : Alternate ports lead to the root bridge, but are not root ports. The alternate ports maintain the STP blocking state.
4. **Backup**: This is a special case when two or more ports of the same bridge (switch) are connected together, directly or through shared media. In this case, one port is designated, and the remaining ports block. The role for this port is backup.

Selection Criteria

Root Bridge Selection

The switch with the lowest Bridge ID is chosen as root.
Bridge ID is a combination of switch priority (32768 by default and the range is 0 to 65535 with increments of 4096) and switch's MAC address

Designated Bridge Selection

i. In a LAN segment, the bridge with the lowest path cost to the Root Bridge will be the DB **OR**

ii. If there are two bridges in the LAN segment with equal path cost to the Root Bridge, then the Bridge with the lowest Bridge ID becomes the DB.

Root Port Selection

i . If there are 2 or more paths to reach the Root Bridge, select the bridge port associated with the lowest accumulated path cost. **OR**

ii. If the path cost to reach the root bridge over 2 or more bridge ports is same, then: select the neighboring switch with the lowest Switch ID value to reach the Root Bridge **OR**

iii. If there are two or more ports on the same bridge with the lowest path cost, then:
* Select the port with the lowest Port Priority value, if you have multiple paths to reach the Root Bridge via same neighbor switch. **OR**
* If all the ports are configured with same priority number (32 by default), select the lowest port number on the switch.

Designated Port Selection

i. The switch port (associated with the DB) on the LAN segment with the lowest accumulated path cost to the Root Bridge will be selected as DP for the given segment. **OR**

ii. If a switch has redundant connections to the network segment, the switch port with the lowest port priority (32 by default) is selected. **OR**

iii. If there is again a tie (it can happen if the priorities of the ports on this switch are the same), then the lowest numbered port on the switch is selected.

Default Timers

Hello----------> 2s
Forward Delay-----> 15s
Max Age----------> 20s

Link Costs

Bandwidth	Cost
10 Mbps---------->	100
100 Mbps---------->	19
1 Gbps---------->	4
10 Gbps---------->	2

Cisco™ CCNA ICND2 : Show Commands

Router Show commands		
Sl. No.	**Command**	**Explanation**
1.	show access-list	Displays all accesslists from all protocols present in a specified router.
2.	show banner	Displays the banner set on the router.
3.	show cdp	Shows the status of CDP such as holdtime value,no.of packets for every 60sec.
4.	show cdp interface	It tells the CDP configuration on an interface-by-interface basis.
5.	show cdp neighbor|detail	Displays info on directly connected neighbors.
6.	show cdp traffic	Displays the CDP traffic info.
7.	show clock	Displays the clock (time, date).
8.	show flash	Used to view all IOS images and file stored in flash(Default location of IOS images is in flash).
9.	show frame-relay lmi	Shows the detailed statistics regarding LMI.
10.	show frame-relay map	Displays the frame relay inverse ARP table.
11.	show frame-relay pvc <dlci_num>	Shows all the frame relay PVC's terminated and their statistics at a specified router.
12.	show history	Shows the previously executed commands.IOS device stores the last ten commands that are executed.
13.	show hosts	Displays the host table.
14.	show interfaces	To view interfaces,status,and statistics for an interface.If u don't lists a specific interface,all of the interfaces on the router are listed.
15.	show ip eigrp neighbors	Shows the list of eigrp neighbors that a specified router has.
16.	show ip eigrp topology	Displays the list of successor and feasible successors,as well as other types of routes.
17.	show ip eigrp traffic	It shows the information about trafiic statistics for eigrp.
18.	show ip interfaces	Displays status and global parameters associated with the interfaces on the router.
19.	show ip interface brief	Displays the interface operational status and IP addresses for all router interfaces.
20.	show ip nat statistics	Displays NAT statistics.
21.	show ip nat translations	Displays the NAT translations.
22.	show ip ospf	Displays general information about OSPF routing processes.
23.	show ip ospf database	Displays lists of information related to the OSPF database for a specific router.
24.	show ip ospf interface	If adjacent router's dont become neighbors, then use the command to check if the local router interface is configured correctly.
25.	show ip ospf neighbor	Displays the OSPF neighbour information.
26.	show ip ospf neighbor detail	Displays all OSPF neighbors in detail.
27.	show ip route	Displays the IP routing table.
28.	show protocols	Displays the routing protocols that have been configured and running on a specified router.
29.	show running-config	Shows the current config stored in RAM.
30.	show sessions	Shows the telnet sessions that are currently suspended.
31.	show startup-config	Shows the configuration stored in NVRAM.
32.	show version	Display version information for the hardware and firmware.
33.	show arp	Displays entries in the ARP table.

Cisco™ CCNA ICND2 : Show Commands

34.	show ip protocols	Displays parameters and current state of the active routing protocol process.
35.	show users	Displays users connected to the router.
36.	show ipv6 interface <interface-name>	Displays ipv6 interface configuration information.
37.	show ipv6 rip	Displays information about all current IPV6 RIP processes.
38.	show ipv6 ospf	Displays general information about OSPF routing processes.
39.	show ipv6 route	Displays routes in the IPV6 routing table.
40.	show ipv6 protocols	Displays parameters and current state of the active IPV6 routing protocol processes.
41.	show ip dhcp binding	Displays IP addresses assigned to the clients.

Switch Show commands		
Sl. No.	**Command**	**Explanation**
1.	show banner	Displays the banner.
2.	show flash	Displays the file contents of the flash.
3.	show history	Displays the last 10 commands entered.
4.	show interfaces	To view interfaces,status,and statistics for an interface.
5.	show interfaces vlan 1	Displays the VLAN status and the IP address of VLAN 1.
6.	show ip interface brief	Verifies the IP configuration.
7.	show running-config	Displays the config held in DRAM.
8.	show startup-config	Displays the NVRAM config.
9.	show users	Displays the users currently logged on.
10.	show version	Display IOS version information for the hardware and firmware.
11.	show vlan	Displays vlan information.
12.	show vlan-membership	Displays vlan membership information.
13.	show mac-address-table	Displays mac-address-table information.
14.	show vtp status	Displays vtp status information such as vtp mode, vtp domain etc.
15.	show spanning-tree	Displays spanning-tree statistics,including information about root bridge and port status.
16.	show spanning-tree summary	Displays summary of port states.
17.	show spanning-tree vlan <vlan-id>	Displays STP information for the specified VLAN.