

1.00	Implement Layer 2 Technologies
1.10	Implement Spanning Tree Protocol (STP)
	(a) 802.1d
	<ul style="list-style-type: none"> - Most popular and widely implemented <p>Steps:</p> <ul style="list-style-type: none"> - Elect root bridge - Determine the root port on each switch - Determine which port will be “designated” for each network segment <p>Bridge ID has two fields: Priority (2 bytes) and MAC address (6 bytes)</p> <p>Priority field is made up of 4-bit priority value and 12-bit “System Extension” (VLAN)</p> <p>Root port is determined by:</p> <ul style="list-style-type: none"> - Root creates “Hello” frame which is sent on the interval set by the hello timer - Each switch modifies the “hello” frame with the cost, the Bridge ID of the forwarding switch, the port priority of the forwarding switch and the port number of the forwarding switch - Hells are not send out ports that are determined to be in “blocking” state - Of all switch ports that receive a hello, the root port is determined by the port with the least calculated cost <p>Default Port Costs – Original (New)</p> <ul style="list-style-type: none"> - 10mb – 100 (100) - 100mb – 10 (19) - 1gb – 1 (4) - 10gb – 1 (2) <p>If there is a tie for cost, the following logic is used to break the tie to elect the root port:</p> <ul style="list-style-type: none"> - Lowest bridge ID - Lowest port priority of adjacent switch - Lowest port number (internally referenced by the forwarding switch) <p>Designated Port</p> <ul style="list-style-type: none"> - This is the port used to forward traffic on the switch that is determined to be “designated” for each LAN segment. - This is the switch with the lowest advertised cost on a particular segment - In case of a tie, same tiebreakers are used as is used to elect the root port <p>Normal “Hello” operation</p> <ul style="list-style-type: none"> - Root switch sends out hello frames based on hello interval schedule - All hellos received are re-forwarded out a switch's designated ports <p>If STP changed, Topology Change Notifications (TCN) are sent and</p>

	<p>forwarded to all switches</p> <p>PVST runs separate STP instance for each VLAN</p> <ul style="list-style-type: none"> - Different VLANs can have different STP trees and thus different paths to destinations - Good way to load-balance over redundant layer-2 links in environments with more than one VLAN - Each VLAN must send BPDUs (significant amount of network traffic) <p>Appropriate SHOW commands:</p> <ul style="list-style-type: none"> - show spanning-tree root - show spanning-tree vlan 1 root detail"
(b) 802.1w	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
(c) 801.1s	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
(d) Loop guard	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
(e) Root guard	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
(f) Bridge protocol data unit (BPDU) guard	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
(g) Storm control	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
(h) Unicast flooding	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
(i) Port roles, failure propagation, and loop guard operation	
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
1.20	Implement VLAN and VLAN Trunking Protocol (VTP)
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
1.30	Implement trunk and trunk protocols, EtherChannel, and load-balance
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
1.40	Implement Ethernet technologies

	(a) Speed and duplex		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(b) Ethernet, Fast Ethernet, and Gigabit Ethernet		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(c) PPP over Ethernet (PPPoE)		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
1.50	Implement Switched Port Analyzer (SPAN), Remote Switched Port Analyzer (RSPAN), and flow control		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
1.60	Implement Frame Relay		
	(a) Local Management Interface (LMI)		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(b) Traffic shaping		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(c) Full mesh		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(d) Hub and spoke		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(e) Discard eligible (DE)		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
1.70	Implement High-Level Data Link Control (HDLC) and PPP		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.00	Implement IPv4		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.10	Implement IP version 4 (IPv4) addressing, subnetting, and variable-length subnet masking (VLSM)		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.20	Implement IPv4 tunneling and Generic Routing Encapsulation (GRE)		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001

2.30	Implement IPv4 RIP version 2 (RIPv2)
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.40	Implement IPv4 Open Shortest Path First (OSPF)
	(a) Standard OSPF areas
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(b) Stub area
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(c) Totally stubby area
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(d) Not-so-stubby-area (NSSA)
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(e) Totally NSSA
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(f) Link-state advertisement (LSA) types
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(g) Adjacency on a point-to-point and on a multi-access network
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(h) OSPF graceful restart
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.50	Implement IPv4 Enhanced Interior Gateway Routing Protocol (EIGRP)
	(a) Best path
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(b) Loop-free paths
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(c) EIGRP operations when alternate loop-free paths are available, and when they are not available
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(d) EIGRP queries
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001

	(e) Manual summarization and autosummarization
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(f) EIGRP stubs
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.60	Implement IPv4 Border Gateway Protocol (BGP)
	(a) Next hop
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(b) Peering
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(c) Internal BorderGateway Protocol (IBGP) and External Border Gateway Protocol (EBGP)
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.70	Implement policy routing
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.80	Implement Performance Routing (PfR) and Cisco Optimized Edge Routing (OER)
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
2.90	Implement filtering, route redistribution, summarization, synchronization, attributes, and other advanced features
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
3.00	Implement IPv6
3.10	Implement IP version 6 (IPv6) addressing and different addressing types
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
3.20	Implement IPv6 neighbor discovery
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
3.30	Implement basic IPv6 functionality protocols
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
3.40	Implement tunneling techniques
	Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
3.50	Implement OSPF version 3 (OSPFv3)
	Not included in sample.

		Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
3.60	Implement EIGRP version 6 (EIGRPv6)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
3.70	Implement filtering and route redistribution	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
4.00	Implement MPLS Layer 3 VPNs	
4.10	Implement Multiprotocol Label Switching (MPLS)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
4.20	Implement Layer 3 virtual private networks (VPNs) on provider edge (PE), provider (P), and customer edge (CE) routers	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
4.30	Implement virtual routing and forwarding (VRF) and Multi-VRF Customer Edge (VRF-Lite)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
5.00	Implement IP Multicast	
5.10	Implement Protocol Independent Multicast (PIM) sparse mode	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
5.20	Implement Multicast Source Discovery Protocol (MSDP)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
5.30	Implement interdomain multicast routing	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
5.40	Implement PIM Auto-Rendezvous Point (Auto-RP), unicast rendezvous point (RP), and bootstrap router (BSR)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
5.50	Implement multicast tools, features, and source-specific multicast	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
5.60	Implement IPv6 multicast, PIM, and related multicast protocols, such as Multicast Listener Discovery (MLD)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.00	Implement Network Security	
6.01	Implement access lists	

Not included in sample.

Buy now at <http://certificationsshortcut.com/study-notes/cisco/350-001>

6.02 Implement Zone Based Firewall

Zone-Based Firewall (ZFW) is also known as “IOS Zone-Based Firewall”

- Router interfaces belong to a security zone
- Traffic can pass between interfaces as long as they are in the same zone
- Traffic cannot pass between zones OR between interfaces that have zones configured and those that have not
- A policy must be configured to allow traffic to pass between interfaces in different zones
- Zone policies configured through “Class-Based Policy Language” (CPL) (similar to MQC)

The following protocols can be inspected and subsequently controlled using ZFW:

- HTTP, HTTPS, SMTP, ESMTP, POP3, IMAP, P2P (including dynamic port configuration), IM applications and RPC

Process to configure ZFW:

- Create the zones you need
- Use CPL to configure the router to identify traffic that must be inspected by using class-maps
- Use CPL to configure the router to assign the policy you wish to enforce on the traffic types defined above
- Use CPL to assign the policy maps to the appropriate zones
- Use CPL to assign the interfaces to the designated zones

Parameter maps can be used to set the inspection behavior for a particular class of traffic within a policy-map. They can also be used for audit trails and alerting functions. Other parameters, such as half-open sessions, can be controlled by parameter maps.

Configuration example:

STEP 1:

- zone security Trusted
 - description Trusted_Zone
- zone security Untrusted
 - description Untrusted_Zone
- zone-pair security Outbound source Trusted destination Untrusted
- zone-pair security Inbound source Untrusted destination Trusted

STEP 2:

- ip access-list extended local_LAN
 - permit ip 192.168.1.0 0.0.0.255 any
- ip access-list extended HTTP_servers
 - permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.1

	<ul style="list-style-type: none"> - permit tcp 192.168.1.0 0.0.0.255 host 10.1.1.2 - class-map type inspect match-all ACME_servers <ul style="list-style-type: none"> - match access-group HTTP_servers - match protocol http - class-map type inspect match-all non_internal_http <ul style="list-style-type: none"> - match protocol http - match access-group name local_LAN - class-map type inspect ICMP <ul style="list-style-type: none"> - match protocol icmp - class-map type inspect Everything_else <ul style="list-style-type: none"> - match access-group name local_LAN <p>STEP 3:</p> <ul style="list-style-type: none"> - parameter-map type inspect timer <ul style="list-style-type: none"> - tcp idle-time 600 - tcp idle-time 600 - policy-map type inspect trusted2untrusted <ul style="list-style-type: none"> - class-map inspect ACME_servers <ul style="list-style-type: none"> - inspect - class-map inspect non_internal_http <ul style="list-style-type: none"> - inspect - class-map inspect ICMP <ul style="list-style-type: none"> - drop - class-map inspect Everything_else <ul style="list-style-type: none"> - inspect timer <p>STEP 4:</p> <ul style="list-style-type: none"> - zone-pair security Internal source Trusted destination Untrusted <ul style="list-style-type: none"> - service-policy type inspect trusted2untrusted - interface f0/1 <ul style="list-style-type: none"> - zone-member security Trusted - interface s0/0/0 <ul style="list-style-type: none"> - zone-member security Untrusted <p>VERIFICATION:</p> <ul style="list-style-type: none"> - show zone-pair security
6.03	Implement Unicast Reverse Path Forwarding (uRPF)
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
6.04	Implement IP Source Guard
	<p>Not included in sample.</p> <p>Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001</p>
6.05	Implement authentication, authorization, and accounting (AAA) (configuring the AAA server is not required, only the client-side (IOS) is configured)
	<p>Not included in sample.</p>

		Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.06	Implement Control Plane Policing (CoPP)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.07	Implement Cisco IOS Firewall	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.08	Implement Cisco IOS Intrusion Prevention System (IPS)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.09	Implement Secure Shell (SSH)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.10	Implement 802.1x	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.11	Implement NAT	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.12	Implement routing protocol authentication	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.13	Implement device access control	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
6.14	Implement security features	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
7.00	Implement Network Services	
7.10	Implement Hot Standby Router Protocol (HSRP)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
7.20	Implement Gateway Load Balancing Protocol (GLBP)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
7.30	Implement Virtual Router Redundancy Protocol (VRRP)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
7.40	Implement Network Time Protocol (NTP)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
7.50	Implement DHCP	

		<p>Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
7.60	Implement Web Cache Communication Protocol (WCCP)	
		<p>Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
8.00	Implement Quality of Service (QoS)	
8.10	Implement Modular QoS CLI (MQC)	
	(a) Network-Based Application Recognition (NBAR)	
		<p>NBAR is “Network-Based Application Recognition”.</p> <p>NBAR makes the classification of packets much easier than it possible without NBAR</p> <p>Challenges addressed by NBAR:</p> <ul style="list-style-type: none"> - Applications using dynamic port numbers (makes it difficult to classify by TCP/UDP port numbers) <p>NBAR inspects packets much deeper and can “see”:</p> <ul style="list-style-type: none"> - Host Name - MIME Type in HTTP - URL - Other application-specific information (via various fields in the packet) <p>NBAR can be used to monitor/log types of traffic and volume of a particular type of traffic that is processed through a device</p> <p>NBAR can assist QoS configurations by allowing the QoS configuration to match particular types of traffic flows that are difficult to match to properly enforce the QoS settings on that type of traffic</p> <ul style="list-style-type: none"> - i.e. using “match protocol” command within QoS configuration <p>One uses for NBAR when configuring QoS is to use NBAR to distinguish between RTP video and audio, which run on different port assignments in the same range of ports</p> <p>NBAR can also distinguish between different Citrix applications even though the traffic is still only Citrix traffic from a pure network analysis perspective</p> <p>Another popular use is to be able to determine which traffic is coming from peer-to-peer (P2P) file sharing applications. It is common to configure your QoS in such a way to put all of this traffic into a “scavenger” class (less than best-effort).</p>
	(b) Class-based weighted fair queuing (CBWFQ), modified deficit round robin (MDRR), and low latency queuing (LLQ)	

		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(c) Classification	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(d) Policing	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(e) Shaping	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(f) Marking	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(g) Weighted random early detection (WRED) and random early detection (RED)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
	(h) Compression	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
8.20	Implement Layer 2 QoS: weighted round robin (WRR), shaped round robin (SRR), and policies	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
8.30	Implement link fragmentation and interleaving (LFI) for Frame Relay	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
8.40	Implement generic traffic shaping	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
8.50	Implement Resource Reservation Protocol (RSVP)	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
8.60	Implement Cisco AutoQoS	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
9.00	Troubleshoot a Network	
9.10	Troubleshoot complex Layer 2 network issues	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
9.20	Troubleshoot complex Layer 3 network issues	
		Not included in sample.

		Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
9.30	Troubleshoot a network in response to application problems	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
9.40	Troubleshoot network services	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
9.50	Troubleshoot network security	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
10.00 Optimize the Network		
10.01	Implement syslog and local logging	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
10.02	Implement IP Service Level Agreement SLA	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
10.03	Implement NetFlow	
		Not included in sample. Buy now at http://certificationshortcut.com/study-notes/cisco/350-001
10.04	Implement SPAN, RSPAN, and router IP traffic export (RITE)	
		<p>SPAN/RSPAN (Switch Port Analyzer / Remote Switch Port Analyzer)</p> <ul style="list-style-type: none"> - Directs all traffic from a port or VLAN to another port for the purposes of monitoring that traffic and possibly acting upon it. - Commonly used to monitor VoIP sessions or to direct traffic to an IDS/IPS solution <p>If destination (monitoring) port is on the local switch, it is considered SPAN If destination (monitoring) port is on a remote switch, it is considered RSPAN</p> <p>With RSPAN, the only difference is the destination is the VLAN created for RSPAN (as opposed to an interface on the local switch)</p> <p>SPAN source ports can be any of the following:</p> <ul style="list-style-type: none"> - Routed port - Physical switch port - Access port - Trunk port - Etherchannel port (one of the physical interfaces or the actual etherchannel itself) <p>When a VLAN is used as the source port, every port on which that VLAN is active is included in the monitoring.</p>

Things to consider/know about SPAN/RSPAN:

DESTINATION:

- When configuring a port as a SPAN destination, the original configuration is lost and is overwritten by the SPAN configuration
- Configuring a port as a SPAN destination removes the port from any Etherchannel bundle if it was originally part of one
- Ports configured as SPAN/RSPAN destinations do not support Dot1x, port security or private VLANs
- Ports configured as SPAN/RSPAN destinations do not support layer-2 protocols including CDP, spanning tree, DTP, VTP, etc.
- Up to 64 destination SPAN ports can exist per switch

OTHER NOTABLE THINGS:

- Source can be VLANs or Physical ports, but not both at the same time
- Be careful not to overload destination ports, especially when the source is a VLAN
- Cannot set up a SPAN and RSPAN destination within the same SPAN session
- Trunks can be configured as a SPAN source. If you only want to monitor certain VLANs, use the “filter VLAN” configuration command
- Traffic ROUTED to a VLAN is not monitored by SPAN – only the physical ports on a switch that have that VLAN configured are monitored
- If you want to capture CDP, BPDUs, VTP, DTP and PagP frames as well (normally not captured), use the “encapsulation replicate” command.

Commands to enable SPAN:

- monitor session 1 source interface Vlan10
- monitor session 1 destination interface f0/4

Commands to enable RSPAN:

MONITORED SWITCH (capturing live data)

- vlan 100
 - remote span
- monitor session 10 source int f0/1 rx
- monitor session 10 destination remote vlan 100

MONITORING SWITCH (has SPAN probe attached)

- vlan 100
 - remote span
- monitor session 20 source remote vlan 100
- monitor session 20 destination interface f0/20

Router IP Traffic Export (RITE) –similar to SPAN or RSPAN but copies IP

	<p>packets to a LAN (or VLAN) interface</p> <ul style="list-style-type: none"> - only includes traffic that hits multiple interfaces simultaneously (commonly used for IDS scenarios) - if traffic is not an attack, it is usually still helpful to see an alert on this behavior to determine exactly what is happening on the network to cause this condition <p>RITE configuration:</p> <ul style="list-style-type: none"> - ip traffic-export profile MyProfile Int f0/0 Bidirectional Mac-address 3324.abcc.d422 Incoming sample one-in-every 50 Outgoing sample one-in-every 25 Int f1/0 Ip traffic-export apply MyProfile
10.05	Implement Simple Network Management Protocol (SNMP)
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.06	Implement Cisco IOS Embedded Event Manager (EEM)
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.07	Implement Remote Monitoring (RMON)
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.08	Implement FTP
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.09	Implement TFTP
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.10	Implement TFTP server on router
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.11	Implement Secure Copy Protocol (SCP)
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.12	Implement HTTP and HTTPS
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>
10.13	Implement Telnet
	<p>Not included in sample.</p> <p>Buy now at http://certificationshortcut.com/study-notes/cisco/350-001</p>

11.00	Evaluate proposed changes to a Network
11.01	Evaluate interoperability of proposed technologies against deployed technologies
	(a) Changes to routing protocol parameters
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(b) Migrate parts of a network to IPv6
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(c) Routing Protocol migration
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(d) Adding multicast support
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(e) Migrate spanning tree protocol
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(f) Evaluate impact of new traffic on existing QoS design
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
11.02	Determine operational impact of proposed changes to an existing network
	(a) Downtime of network or portions of network
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(b) Performance degradation
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(c) Introducing security breaches
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
11.03	Suggest Alternative solutions when incompatible changes are proposed to an existing network
	(a) Hardware/Software upgrades
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001
	(b) Topology shifts
	Not included in sample. Buy now at http://certificationsshortcut.com/study-notes/cisco/350-001

	(c) Reconfigurations
	Not included in sample. Purchase complete 350-001 exam notes