IDG .com

NETWORKWORLD® Reprint

The leader in network knowledge ■ www.networkworld.com September 5, 2005 ■ Volume 22, Number 35

CLEAR CHOICE TEST

10 GIGABIT ETHERNET SWITCH

CATALYST 4948-10GE

Cisco www.cisco.com

NetResults 4.75

$30,000 as tested.

Pros: Low latency and line-rate throughput; innovative security features.

Cons: Pricey; not expandable; unique X2 transceivers might increase sparing costs; no IPv6 support.

The Breakdown

L2 switching performance	15%	5
L3 switching performance	15%	5
VLAN switching performance	15%	5
OSPF switching performance	15%	5
Security	20%	5
Features	20%	3.75
Total score		**4.75**

Scoring Key:
5: Exceptional.
4: Very good.
3: Average.
2: Below average.
1: Subpar or not available.

Cisco Catalyst 4948-10GE aces performance tests

BY DAVID NEWMAN, NETWORK WORLD LAB ALLIANCE

In an exclusive *Network World* test, Cisco's Catalyst 4948-10GE delivered record low latency and line-rate throughput. Coupled with innovative security mechanisms and an extensive list of switching and routing features, this switch earns a Clear Choice award.

With a price of $30,000, the Catalyst 4948-10GE is too costly to be deployed in every wiring closet, but the price makes sense for use in data centers where the switch can aggregate connections from many servers and send traffic over a 10-Gigabit Ethernet backbone.

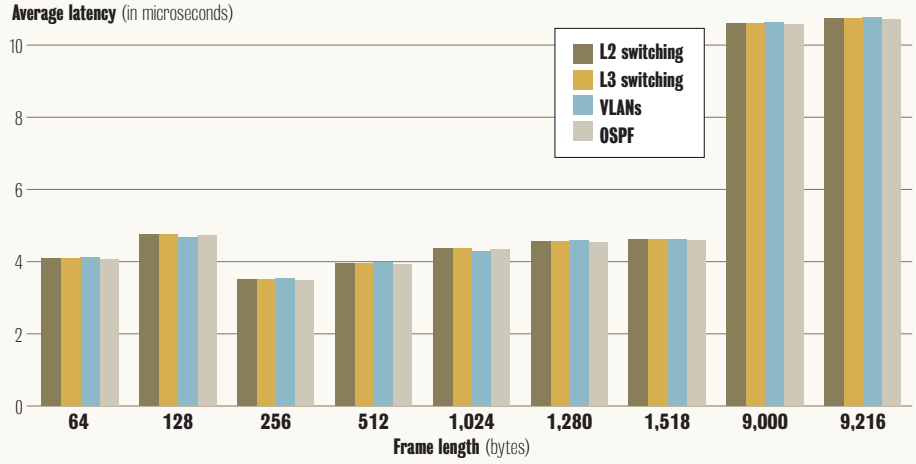
The Catalyst 4948-10GE offers 48 copper Gigabit Ethernet and two 10G Ethernet ports, much like competing products from Extreme Networks, Force10 Networks and Foundry Networks. There are some key differences, though: The Cisco switch has a 1-rack unit (1.75-inch) form factor, while Foundry's FESX448 occupies 1.5 rack units. The Cisco switch supports redundant power supplies, while redundancy for Extreme's S400-48t requires one external power supply (however, Extreme's external power supply can be shared across multiple switches). On the downside, Cisco's device is not expandable, unlike Force10's S50, and its list price is higher than similarly configured competitors' switches.

Perhaps the biggest difference is Cisco's use of X2 transceivers for 10G Ethernet interfaces. These are roughly the size of Gigabit Ethernet transceivers, putting them about halfway between 10G Ethernet Transceiver Package (XENPAK) transceivers and smaller 10 Gigabit Small Form Factor Pluggable transceivers (XFP) in newer 10G switches from Force10, Foundry and Nortel, among others. One consideration for adopters of multiple transceiver types is that they'll have to keep multiple types of spares on hand, with prices well into the thousands of dollars for each.

X2 transceivers are functionally identical to XENPAK transceivers, while XFP transceivers offload the serializer/deserializer (Serdes) function to the switch's circuit board. Cisco says X2s boost reliability because a Serdes failure requires replacement of just a transceiver rather than an entire switch. We're not sure about that claim: While it's still relatively early for XFPs, we've yet to junk an XFP device because of a Serdes failure. We did verify that X2 transceivers interoperate with

Cisco's Catalyst 4948-10GE is low on latency

On average, the Catalyst 4948-10GE held up traffic on 10-Gigabit Ethernet interfaces only around 4 microseconds for most frame lengths. That's the lowest latency we've recorded for any 10-Gigabit Ethernet switch we've tested.



both XENPAK and XFP transceivers over single-mode fiber cabling.

Peak performance

We stress-tested the Catalyst 4948-10GE in various configurations, and it came up aces in all of them. These configurations involved Layer-2 and -3 switching, virtual LANs (VLAN) and Open Shortest Path First (OSPF) routing, all common tasks for an aggregation switch. We also measured the switch's buffering and unicast address learning capacity.

We pounded the switch with a traffic pattern that involved fully meshed traffic between all 48 Gigabit Ethernet ports, as well as traffic between the two 10G Ethernet ports (see How we did it). No production network (hopefully) ever sees traffic like this, but it does allow us to determine the limits of system performance.

The Layer-2 and -3 switching tests were simple, with only one media access control (MAC) and/or IP address per port. For the VLAN tests, we defined 28 VLANs on each Gigabit Ethernet port, for a total of 1,344 VLANs. For the OSPF tests, we used the Spirent SmartBits traffic generator/analyzer to emulate 10,000 networks with 250 hosts on each. Because this last test involved 2.5 million flows, it's a good way to determine if performance degrades as flow count rises.

In all tests, the Catalyst 4948-10GE delivered line-rate throughput of up to 101.19 million frames per second.

We also measured latency — the time needed by the switch to forward each frame at the throughput rate (see graphic, front). Average latency hovered in the range of 4 microsec for most frame lengths, a new low among Ethernet switches we've tested. All latency numbers we recorded are at least one order of magnitude below the point where they would affect even the most time-sensitive application. Latency and jitter were also remarkably low and constant for the Gigabit Ethernet interfaces.

We also measured the switch's buffering capacity, or how long it holds up traffic when it's overloaded. With both two-to-one and 10-to-one overloads, the maximum delay we observed was about 1.4 millisec for 64-byte frames; 26 millisec for 1,518-byte frames; and 128 millisec for 9,000-byte frames. None of these worst-case results are likely to degrade application performance in production networks.

Cisco says the Catalyst 4948-10GE can keep track of 55,000 unicast MAC addresses without flooding. We verified that claim by offering 54,999 addresses of our own, which, added to the switch's own address, matches the data-sheet claim.

Security features

The Catalyst 4948-10GE has a well-stocked security arsenal. Like many other switches, it supports 802.1X user authentication, Secure Shell v2 for remote access, and access control lists. The switch offers many other security features, as well.

The port security feature allows the switch to learn the MAC addresses of attached hosts, even across reboots, preventing spoofing and boosting reliability.

DHCP snooping enables the switch to listen for and reject responses from rogue DHCP servers, thus preventing an attacker from misconfiguring hosts and redirecting traffic. DHCP snooping also can rate-limit traffic to legitimate DHCP servers, preventing denial-of-service attacks.

The IP source guard feature builds on DHCP snooping to prevent an attacker from using a legitimate user's IP address to inject spoofed traffic. The device builds a table that associates IP addresses with switch ports. If an attacker tries to send traffic with a source IP address already registered to another port, the switch drops the traffic.

Both DHCP snooping and IP source guard both work on 802.1Q trunks, 802.3ad link aggregation trunks (or Cisco EtherChannels), and private virtual LANs, as well as on individual ports.

The Dynamic ARP inspection (DAI) feature blocks attackers from using Address Resolution Protocol (ARP) cache poisoning, a relatively easy and common exploit for many other switches and routers. By sending gratuitous ARP messages to many switches and routers, an attacker can redirect traffic to and from a legitimate user's IP address, thus capturing passwords, e-mail, VoIP calls or any other traffic. DAI thwarts this attack by maintaining a table of IP-MAC bindings, and dropping traffic to MAC addresses not listed in the binding table.

Our only complaints with the Catalyst 4948-10GE are minor: Is relatively high list price (often discounted in large deals); its lack of expandability; the possible need to stock multiple 10G transceiver types; and its lack of IPv6 support (which isn't yet a requirement for many network managers, anyway). In every other respect, the switch is a standout. It brings line-rate throughput, minimal latency and innovative security features to data center networks.

Newman is president of Network Test, an independent engineering services consultancy in Westlake Village, Calif. He can be reached at dnewman@networktest.com.

Thanks

Network World *gratefully acknowledges the support of Spirent Communications, which supplied its SmartBits traffic generator/analyzer system.*

How we did it

We assessed the Catalyst 4948-10GE in terms of performance, security and features. We tested performance in six areas: throughput/latency in L2, L3, Open Shortest Path First and virtual LAN configurations; buffering capacity during congestion; and unicast MAC address capacity.

To test throughput and latency, we configured a Spirent SmartBits traffic generator/analyzer to offer traffic to all 48-Gigabit Ethernet switch ports in a fully meshed traffic pattern, while simultaneously offering traffic to both 10 Gigabit Ethernet switch ports in a port-pair traffic pattern. We repeated this test with nine Ethernet frame lengths: 64-, 128-, 256-, 512-, 1024-, 1280-, 1518-, 9000-, and 9216-byte frames. In all cases, we configured Spirent's TRT Interactive 5.0 application to offer traffic for 60 seconds, and recorded throughput and average latency measurements.

We ran these tests with the Catalyst 4948-10GE in L2 (bridging) and L3 (IP forwarding) configurations. We then enabled 1,344 virtual LANs on the Catalyst 4948-10GE (28 per Gigabit Ethernet port) and reran the same traffic pattern. We also tested with OSPF enabled. In the OSPF tests, we established one adjacency with each Gigabit Ethernet interface and advertised a total of 10,000 networks and offered traffic to 250 hosts on each network, for a total of 2.5 million flows.

To measure buffering capacity, we offered traffic at line rate to two Gigabit Ethernet switch ports, both destined to the same output port. We measured delay on the output port to determine buffer capacity. We then repeated the same test with a 10-to-1 overload.

To determine MAC address capacity, we used Spirent's SmartWindow application to offer various numbers of addresses in learning and test phases as described in RFC 2889.