

PACKET

CISCO SYSTEMS USERS MAGAZINE

SECOND QUARTER 2005

SELF-DEFENDING NETWORKS

Network Security Evolves to Eradicate Attacks at Their Source 26

Designing the Data Center Access Layer 57

Wideband Protocol for DOCSIS 19



CISCO SYSTEMS

CISCO.COM/PACKET



Safe Metro Aggregation

Innovative Catalyst switch and QoS features bring security, reliability, resilience, and high performance to the metro aggregation layer.

By Rupa Kaur

The Metro Ethernet market is undergoing explosive growth, and security is extremely important at the metro network's entry location. Modular Cisco Catalyst switches are used to terminate multiple DSL access multiplexers (DSLAMs) at the aggregation layer. DSLAMs are intelligent devices and support multicast Internet Group Management Protocol (IGMP) snooping for triple-play voice, video, and data services. They also support Dynamic Host Control Protocol (DHCP) interface tracking (Option 82) and isolation for end subscribers.

DSLAMs, however, do not offer security features such as dynamic protection from man-in-the-middle attacks, IP spoofing, and DHCP denial-of-service (DoS) attacks. These functions with innovative quality-of-service (QoS) features are performed at the metro aggregation switching layer. Generally, in this topology each DSLAM connects to a Cisco Catalyst switch using two Gigabit Ethernet interfaces (see Figure 2, page 62).

Catalyst 4500 with Supervisor Engine V-10GE

A wire-speed 10 Gigabit Ethernet-enabled Cisco Catalyst switch is a de facto choice for service providers, because it allows them to offer high-bandwidth, rich services that will satisfy customers and keep the service providers competitive. Performance of up to 136-Gbit/s switch capacity and 102 million packets per second (pps) of wire-speed forwarding are supported on a single Cisco Catalyst 4500 Series Switch with a Supervisor Engine V-10GE. Modular supervisors support a full range of 4096 active virtual LANs (VLANs) in accordance with IEEE 802.1q. In addition, none of the services suffer a performance penalty, because they are performed in hardware—allowing providers to offer a greater number of Metro Ethernet point-to-point or point-to-multipoint Ethernet services.

The bidirectional Ethernet (100BaseBX, 1000BaseBX) interfaces in the Catalyst 4500 Series Switch implement full duplex, wire-speed, Fast or Gigabit Ethernet point-to-point services on a single fiber cable. The GLC-BX-U (upstream, customer end) and GLC-BX-D (downstream, service provider) Small Form-factor Pluggable (SFP) interfaces are supported on the switch's Gigabit Ethernet ports. These interfaces provide additional return on investment (ROI), decreasing the cost of underground dark fiber by half. The new bidirectional SFPs are installed in pairs (blue + purple on each end), and each SFP carries a different wavelength. Common deployments include the bidirectional SFPs terminating subscribers on switch downlink connections and 2x10GE line rate uplinks to the Cisco 7600 Series Router in the Metro Ethernet core.

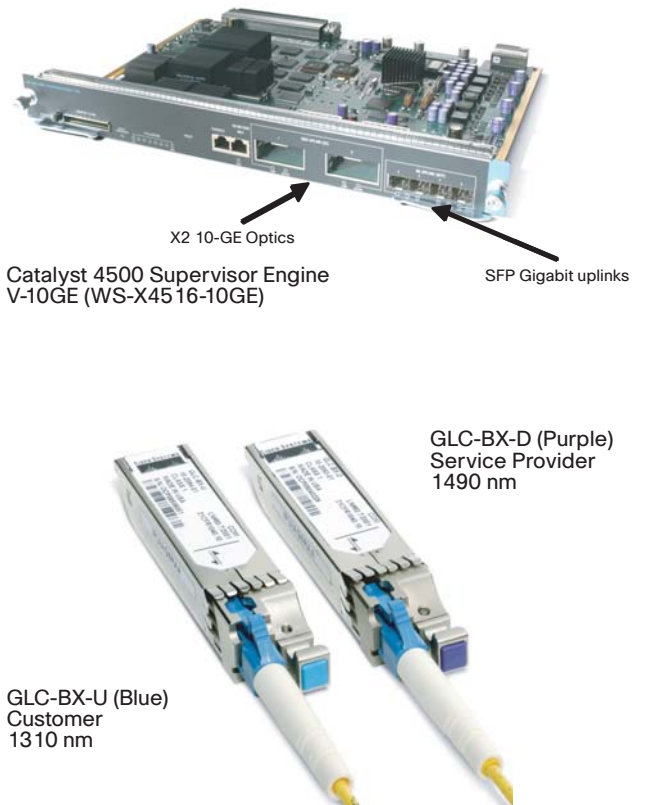


FIGURE 1 New security and quality-of-service features supported by the Cisco Catalyst 4500 Series Switch bring greater performance and protection to metro aggregation deployments. Bidirectional Gigabit Ethernet interfaces can lower the cost of underground dark fiber by half.

New Security and QoS Features in Catalyst Switch

Several new security and QoS features for the modular Cisco Catalyst switches bring a comprehensive security portfolio to metro aggregation deployments and allow network managers to dynamically control security threats at their inception. These tightly integrated software and hardware features work together and can be simultaneously deployed on a switch.

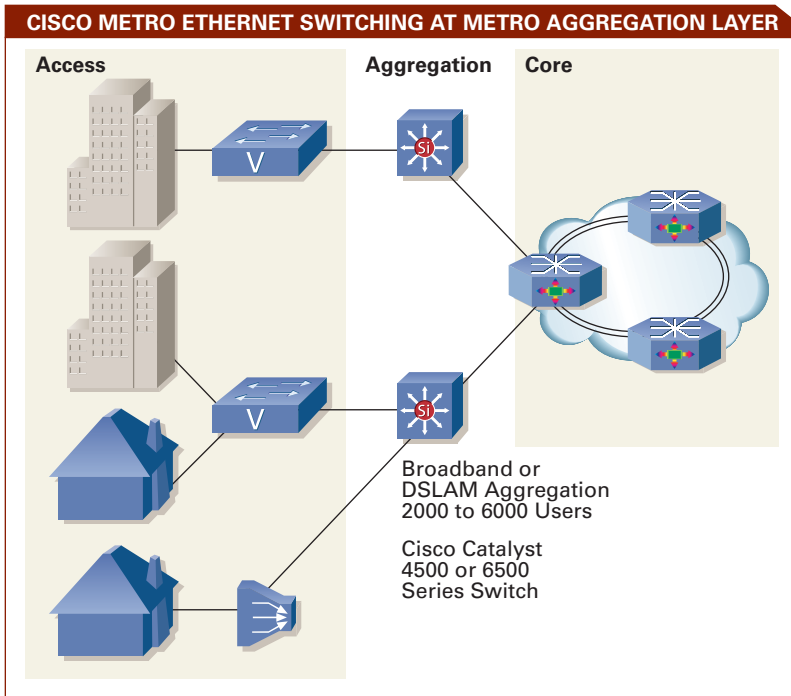


FIGURE 2 Security features—such as dynamic protection from man-in-the-middle attacks, IP spoofing, and DHCP DoS attacks—are performed by the Catalyst switch at the metro aggregation layer.

- **Private VLAN (PVLAN) trunk ports** allow content and media (data, voice, video) distribution to homes from different service providers over the same infrastructure. The trunk ports can carry multiple isolated and regular VLANs and also provide isolation between different ports on downlink connections. This feature simplifies IP address management by keeping all clients on the same IP subnet. PVLAN trunk ports enhance security by providing isolation between the ports and eliminating spoofing attempts of services across subscribers.
- **Promiscuous PVLAN trunks** carry multiple VLANs on uplink trunk ports connected to the router. This security feature also maintains isolation between subscribers carried over the same trunk and simplifies network implementation across the wirespeed 10 Gigabit Ethernet uplink ports.
- **Trunk port security** mitigates MAC spoofing attempts on an inter-switch link (ISL) or 802.1q trunk port. A Catalyst switch can be configured to limit MAC addresses with a per port per VLAN emphasis. This approach prevents various MAC table exhaustion attacks.
- **Per port per VLAN QoS (PVQoS)** is a new feature for input and output QoS. Prior to this feature, a Catalyst switch could only be used for either port level or VLAN level QoS, but not both. This feature allows a metro service provider to customize its own granular QoS service policy per VLAN on any port to better differentiate service offer levels. Multiple service policies for each VLAN are also supported on any given port.

- **8000 input and 8000 output policers** are supported for concurrent input and output policing with PVQoS. This feature allows a service provider to fine tune traffic traversing ingress and egress ports to thousands of subscribers.
- **Aggregation DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard** to dynamically prevent DHCP, man-in-the-middle, and IP spoofing attacks, respectively. These re-engineered security features now allow providers to enable security policies on a DHCP packet even when DHCP interface tracking (Option 82) is performed at the DSLAM level. Prior to this enhancement, these dynamic Layer 2 security features could only be used for metro access deployments, e.g., in a building basement without DSLAMs.
- **Hardware Ternary CAM 3 (TCAM)** is used to look up one or more matching bits in the incoming packets and classify them for different features, such as security ACLs and QoS classification. The set of bits and its value to match is programmed in a TCAM entry, and the set of bits to be considered for matching is programmed in a TCAM mask. In TCAM3, there is one-to-one correspondence between a TCAM entry and TCAM mask, whereas in earlier versions, there are eight TCAM entries for a given mask. Because the new TCAM has more TCAM entries utilization than previous TCAMs, it allows for more security and QoS classification rules.

In addition, with the TCAM3 hardware interface, packet lookup is performed at wirespeed by the switching engine ASIC. These TCAMs also make it possible for Catalyst switches to process security services on any range of IP address in hardware. Because of the one-to-one correspondence between a TCAM entry and its mask, the TCAM3 is amply equipped to meet the future needs of metro aggregation security and QoS features. Even when classifying flows from 6000 different IP addresses and all dynamic aggregation security features, the TCAM entry utilization is only 10 percent.

Figure 3 shows the applicability of these new features within a metro aggregation network. The topology is included to the extent that specific security features should be requested to mitigate the effects of certain attacks.



RUPA KAUR, a senior technical marketing engineer in the Gigabit Switching Business Unit, has been at Cisco ten years. Before her role in technical marketing, she was a development engineer for ATM platforms. She can be reached at rupa@cisco.com.

```

Policy-map P31_QoS // A 200 Mbps policer definition
Class RT
Police 200m 16k conform transmit exceed drop // Up to 8K in & 8K out policers

interface range GigabitEthernet3/1-48 // Sample Downlink ports
switchport trunk encapsulation dot1q
switchport private-vlan trunk native v1an 401
switchport private-vlan association trunk 200 201 // PVLANS secondaries as services
switchport private-vlan association trunk 300 301 // PVLANS secondaries as services
switchport mode private-vlan trunk // Private v1an isolated trunk
switchport port-security // Enable port security
vlan-range 201 // PVQoS and trunk port security
port-security maximum 3
  service-policy input P31_QoS // Ingress PVQoS for VLAN 201 (includes policing)
  service-policy output P31_QoS // Egress PVQoS for VLAN 201 (includes policing)
vlan range 202
port-security maximum 3
  service-policy input P32_QoS // Ingress PVQoS for VLAN 202 (includes policing)
  service-policy output P32_QoS // Egress PVQoS for VLAN 202 (includes policing)
spanning-tree portfast trunk

interface range tengigabitethernet1/1-2 // Uplink ports
switchport mode private-vlan trunk promiscuous // PVLAN promiscuous trunks

```

FIGURE 4 Sample configuration for ingress/egress policing, trusting DSCP, and giving precedence to voice packets on a Cisco Catalyst 4500 Series Switch.

PVLANS are extremely useful in a Metro Ethernet environment because they automatically provide isolation between multiple DSLAMs. PVLAN isolated trunks are used to multiplex several VLANs on the same port while still maintaining isolation between subscribers. The feature also allows a customer to subscribe to multiple ISPs with transparent networks. The PVLAN promiscuous trunks (2HCY2005) are used to carry services for thousands of subscribers on the switch's uplink ports. Prior to promiscuous trunks, a Catalyst switch could only carry one VLAN on a promiscuous port, thus requiring a greater number of physical ports. With this new feature, many primary PVLANS can be multiplexed onto one or both (resilient and load sharing) 10 Gigabit Ethernet or Gigabit Ethernet uplinks. The PVLAN promiscuous trunks on the Catalyst 4500 connect to the Cisco 7600 Series Router where IPv4, IPv6, or Multiprotocol Label Switching (MPLS) services are performed.

Trunk port security is also supported on PVLAN trunk ports. It restricts the allowed MAC addresses or the maximum number of MAC addresses to individual VLANs on a trunk port. It restricts the trunk port to configured MAC addresses so no other MAC address can join the network. When a trunk port security violation occurs, the trunk port is shut down and a Simple Network Management Protocol

(SNMP) trap might be generated. Trunk port security can be used when a Catalyst switch has an 802.1q or ISL trunk attached to a neighboring Layer 2 switch or DSLAM.

Per port per VLAN QoS allows network managers to create their own service policy per VLAN. This policy, performed in hardware, might consist of ingress and

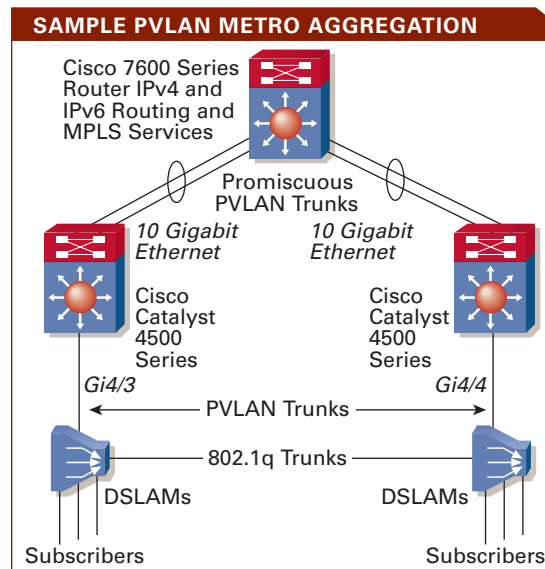


FIGURE 3 Security features, such as PVLAN, on Cisco Catalyst modular switches allow network managers to dynamically control security threats at their inception.

FIGURE 5 Sample configuration for DHCP Snooping on a Cisco Catalyst 4500 Series Switch.

```
Switch#show ip dhcp snooping binding interface Gi4/1
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:09:6B:50:B8:28	10.33.235.45	131585	dhcp-snooping	201	GigabitEthernet4/1
00:02:B9:A7:55:A5	10.33.232.47	439124	dhcp-snooping	200	GigabitEthernet4/1

FIGURE 6 Sample configuration for Dynamic ARP Inspection and IP Source Guard on a Cisco Catalyst 4500 Series Switch.

```
ip dhcp snooping allow-untrusted // Option 82 Passthrough
ip dhcp snooping // Enabling dhcp snooping and activating it on vlans 2-10
ip dhcp snooping vlan 2-10
ip arp inspection vlan 2-10 // Enabling Dynamic ARP Inspection on vlans 2-10
interface range gi2/1 - 48 // DHCP and ARP DoS attack rate limiters (in pps)
ip dhcp snooping limit rate 200
ip arp inspection limit rate 200
ip verify source vlan dhcp-snooping port-security // IP source guard
```

egress policing, trusting Differentiated Services Code Point (DSCP), or giving precedence to voice packets over data. Figure 4 shows a sample configuration for these three features on a Cisco Catalyst 4500 Series Switch.

DHCP interface tracking, or Option 82, satisfies the legal requirements of many countries, which stipulate that DSLAMs constantly track the DHCP offers and releases. DHCP interface tracking only provides a tracking path for the DHCP packet but does not enforce security. The DSLAM inserts information about itself in the DHCP request packet traversing from a client to a server. When a Catalyst switch is used in aggregation mode, it cannot change the Option 82 coming from DSLAMs, forcing the port to be trusted. Trusting the port rendered the industry-leading DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard security features to be unavailable for Metro Ethernet. Today, Cisco has re-engineered the Catalyst switch for Option 82 passthrough, which means that the switch transparently passes Option 82, enabling deeper inspection of the DHCP packets.

DHCP Snooping combats rogue DHCP servers while protecting the network from DoS attacks. It achieves this by rate limiting the incoming DHCP packets and limiting client-facing ports for sending DHCP request and renew traffic only. The edge ports, for example, cannot offer DHCP lease, which is a function for the DHCP server. DHCP Snooping also forms the basis for other security features such as IP Source Guard and Dynamic ARP Inspection. This feature allows the switch to “snoop” the switching traffic for DHCP packets and create a dynamic binding (see Figure 5).

Dynamic ARP Inspection uses the DHCP Snooping bindings to prevent ARP spoofing and man-in-the-middle attacks for both static and dynamic IP addresses. Any violating hosts can be logged and the ports error-disabled until an administrative action is taken. IP Source Guard mitigates IP address spoofing by dynamically maintaining per port VLAN ACLs. IP Source Guard adds security to IP source address using DHCP Snooping table. The feature automatically locks an IP and MAC address to a given port. The dynamic ACL is removed when the user releases the IP address, for example, with “ipconfig /release.” Figure 6 shows a sample configuration for these features.

All the Cisco Catalyst security and QoS features discussed in this article build on one another—much like a set of security “stairs” upon which all services are deployed concurrently. These security features empower service providers with resilient, high-performance, reliable, and secure metro Layer 2+ networks. The switches are not only built for the needs of today’s networks but are well equipped to meet the demands and challenges of tomorrow. ■

FURTHER READING

- Cisco Catalyst 4500 Series Supervisor Engine V-10GE cisco.com/packet/172_8a1
- Cisco Metro Ethernet Switching Solution for Service Providers cisco.com/packet/172_8a2