

Deploying Metropolitan Ethernet Services: Features and Technologies Essentials

Introduction

Today's service providers are faced with numerous customer opportunities. While large enterprise customers will typically use dark fiber to build out their own metro networks, many mid-tier and small businesses are looking for the ideal metropolitan-area network (MAN or metro) interconnect technology to propel them beyond the T1/E1 bandwidth bottleneck, while supporting their converged infrastructure for data, voice, and video services. In the meantime, residential users are primarily interested in high-speed broadband services that provide voice, video (such as Video on Demand), and Internet access.

Service providers are looking to address the needs of their customers by providing innovative and flexible service solutions. Providers in the business of supporting enterprise customers need to maintain their existing, profitable WAN services while at the same time providing Ethernet-based, bandwidth-enhanced WAN services for customers that need more than what's offered by today's existing circuit-based offerings. Providers that offer residential and small-business services must build and deliver cost-effective, high-quality solutions that exceed today's limited ability to deliver high-quality voice, video, and data to end users.

The Cisco Metro Ethernet switching portfolio provides an ideal solution and foundation for providers to offer unique services to both residential and business users. These capabilities include industry-leading resiliency, quality of service, security, VPN, and voice/video services. This document explores the technologies that enable service providers with the tools to build metro network solutions and offer profitable services which are highly desirable to their customers.

Cisco Service-Enabling Capabilities For Metropolitan Networks

Cisco leads the industry in providing high performance switching platforms. With the Cisco Internetwork Operating System (IOS), Cisco delivers a wide variety of features and functionality that service providers need. These features include capabilities to make their networks resilient, offer differentiated traffic classes to their customers, secure their networks and protect their customer's traffic. The Cisco Metro architecture and solutions therefore allows providers to offer unique services to their customers, including VPN services for business and voice/video services for residential users. These features and technologies demonstrate the robustness of Cisco IOS® Software and its support of innovative, leading-edge features and services designed to enhance metro services.



Service Resiliency and Reliability

Enterprises understand more than ever how important network resiliency is to their ongoing viability. Having robust backup systems gives businesses the confidence to address any interruptions. Both service providers and their end users benefit when deployed solutions offer exceptional levels of service reliability and resiliency. Cisco IOS® Software, Cisco routers, and Cisco Catalyst® switching platforms offer the highest level of redundancy and fault tolerance through extensive hardware and software system features. The end result is a network infrastructure engineered with multiple layers of protection mechanisms, creating a safety net designed to repair the network infrastructure even after the most catastrophic network failures.

The following is a list of high-availability features, which benefit metro customers.

- 1 + 1 supervisor redundancy support (Cisco Catalyst 6500 and 4500 Series Switches and Cisco 7600 Series Internet Router)
- 2-3 second Stateful Supervisor Failover Support (Catalyst 6500 and Cisco 7600)
- Stateful Layer 3 Forwarding, Spanning Tree, CAM Tables, ACLs, QoS, Port Security (MAC Based & 802.1x), and WAN Interfaces (Catalyst 6500 and Cisco 7600 Internet Router)
- 1 + 1 power supply redundancy support (Catalyst 6500, 4500, Cisco 7600 Internet Router and the Cisco RPS 300 backup power-supply solution for the Cisco Catalyst 3550)
- Redundant switching fabric support (Cisco Catalyst 4500 and 6500 Series Switches and Cisco 7600 Series Internet Router)
- Advanced spanning-tree features (Root and BPDU guard, PVST+, 802.1s/802.1w, PortFast, UplinkFast and BackboneFast, and Loop Guard))
- Hot Standby Routing Protocol (HSRP)
- EtherChannel® support at 10, 100, 1000 Mbps, and 10 Gbps (up to 16 Gbps of aggregation and a bundle of up to 8 ports)

For service providers, these reliability and resiliency features translate to peace of mind over the sustainability of customer service-level agreements (SLAs). To end users, these features help ensure productivity and profitability that could be greatly affected in the face of network instability.

Quality of Service

In order for service providers to effectively manage their bandwidth usage and offer tiered traffic service levels, they must implement an intelligent quality of service (QoS) strategy that provides extensive traffic prioritization and policing options beyond what is available through a basic hardware queue model approach.

Cisco Metro Ethernet solutions take full advantage of the unparalleled traffic prioritization and policing options offered by Cisco IOS® Software. The intelligent traffic policing and prioritization features that are offered as part of Cisco Metro Ethernet solutions are:

- Per-port QoS Access Control List (ACL) configuration
- Weighted Round Robin (WRR) scheduling
- Weighted Random Early Detection (WRED) congestion management
- Strict priority queuing
- IP Differentiated Services Code Point (DSCP) and IP Precedence



- Per-packet reclassification and marking based on:
 - IP Type of Service (ToS or DSCP)
 - Complete Layer 3 and 4 headers (IP only)
- Input/output policing based on Layer 3 and 4 headers (IP only)
- Support for 1024 ingress and 1024 egress policers (configurable as aggregate or individual)
- No performance penalty for highly granular QoS functionality
- OSM/FlexWAN QoS Support (Class Based Weighted Fair Queuing (CBWFQ)/Low Latency Queuing (LLQ) and shaping)

This robust suite of QoS features provides unmatched network traffic management intelligence to ensure that network traffic is classified, prioritized, and scheduled in an optimal way, efficiently servicing bandwidth-hungry, time-sensitive applications, including voice, video, and other mission-critical traffic.

Security

Just as unauthorized network-access cases are on the rise, the methods being used to perpetrate these break-ins are becoming more technically sophisticated. Unauthorized access to a customer's data or systems as a result of poor network security precautions can result in a loss of provider credibility, and potentially a loss of productivity or worse for the customer. Network service providers and their customers require a comprehensive security solution to keep these unwanted breaches at bay.

By using the rich blend of network traffic security options available in Cisco IOS® Software, Cisco Metro Ethernet solutions are inherently able to offer security configuration options that meet both service-provider and end-customer needs. Some of the security features that are part of the Cisco Metro Ethernet solution portfolio are listed below:

- Terminal Access Controller Access Control System (TACACS+) and Remote Authentication Dial-In User Service (RADIUS)
- 802.1x dynamic port-based user authentication
- Cisco 802.1x Extensions (802.1x with VLAN, 802.1x Guest VLANs, 802.1x & Port Security, and 802.1x with AVVID)
- Router ACLs (Standard/Extended ACL support On All Ports)
- Virtual LAN (VLAN) ACLs (Standard/Extended ACL support On All Ports)
- Dynamic Host Configuration Protocol (DHCP) snooping (Cisco Catalyst 4500 Series)
- Port security
- Private VLANs and Private VLAN Edge

Another recently introduced security feature for metro service providers is DHCP Interface Tracker (Option 82). The DHCP Interface Tracker feature involves the interception and modification of DHCP requests made by clients attached to Cisco Catalyst 3550 and 4500 series switching platforms. The modification of these DHCP server-bound requests involves the addition of an identifier, which describes the switch and the port where the request originated. Appending this descriptive information provides an identification mechanism that can be used for the following purposes:

- Basic authentication (*Should the requesting port be serviced?*)
- IP address management (*How many IP addresses should the DHCP server grant the requesting port?*)



- Port/IP/MAC binding for policy, application, and access management (*Should the requesting port be given access to an application based on the policy governing it?*)

Specific to service providers, DHCP Interface Tracker can be used as a way to control access to specific applications and services using access leases or licenses, which are typically governed by a license or policy server.

Robust Multicast for Voice and Video Services

As demand increases for high-speed multimedia traffic, service providers must address the need to offer scalable voice and video services to their customers. Applications, which are driving this demand, include digital television (MCTV), video on demand (VOD), and large-scale IP-based telephony services. Generic multicast solutions are incapable of scaling to a level suitable for residential usage, which would impose an excessive bandwidth and processing burden on provider network gear due to inherent multicast design inefficiencies with large-scale deployments.

To efficiently deal with the mass delivery of these emerging media types, service providers need an innovative multicast feature suite that goes beyond the typically offered feature set and addresses the unique needs of mass residential deployments of high-quality voice and video services.

Cisco IOS Software meets this need by offering a diverse set of multicast features and technologies designed to enable service providers to deliver large-scale distribution of subscriber-based, time-sensitive traffic feeds to their customers. Some of the innovative multicast features offered by Cisco IOS Software include:

- Protocol-Independent Multicast (PIM)—Sparse and Dense modes
- Distance Vector Multicast Routing Protocol (DVMRP) tunneling
- Interior Gateway Multicast Protocol (IGMP) snooping
- Internet Group Management Protocol (IGMP) filtering
- Voice VLAN

Multicast VLAN Registration (MVR) is another innovative feature that is key for metro service providers interested in delivering residential voice and video services. MVR involves the creation of separate dedicated VLANs constructed specifically for multicast traffic distribution. When deployed, each Cisco Catalyst switch that receives an MVR stream will examine each multicast group and will internally bridge the multicast VLAN traffic to the particular subscriber's VLAN. Cisco Catalyst 2950 and 3550 series support MVR.

Virtual Private Network Services

Businesses today are faced with a major dilemma—how to securely connect a growing number of employees—many of whom are mobile—while maintaining or reducing the cost of their communications infrastructure. Further burdening this issue is the emergence of electronic business practices involving outside business partners and vendors and the need to connect to these groups to foster communication. A logical solution is virtual private network (VPN) technology.

VPNs allow corporations to use the Internet for all their secure communication needs. Whether connecting remote offices, offering remote access to traveling employees, or connecting with business partners, VPNs securely extend corporate networks and reduce the costs that are incurred by leased lines and Frame Relay networks.



For service providers, VPN service offerings have the potential to be a major source of revenue. With the increase in the mobility of today's workforce and the universal need for corporations to limit their communications costs, VPN services offer most customers an attractive solution that effectively addresses both of these trends.

Cisco Metro Ethernet solutions take advantage of the entire suite of VPN features inherent in Cisco IOS® Software. As a result, Cisco is able to offer comprehensive VPN feature support across the entire Cisco router and Cisco Catalyst switching product portfolio.

One challenge that can affect the cost-effectiveness of provider VPN solutions involves the routing functionality and tunnel termination associated with VPNs deployed in areas with a large number of densely populated buildings. In a typical Multiprotocol Label Switching (MPLS) VPN scenario, every customer has its own dedicated customer-edge device, with a dedicated connection to the local provider-edge switch. MPLS VPNs typically terminate at a dedicated customer port on the provider-edge device, where the VPN-associated routing intelligence resides. Each of the dedicated ports on the provider-edge device is then connected directly to the specific customer's switch. This one-to-one association inefficiently consumes costly ports on the provider edge and can rapidly consume available device port density.

To solve this problem, Cisco has developed Multi-VPN Routing and Forwarding (Multi-VRF). Multi-VRF is a Layer 3 enhancement that allows multiple VPN customers to share a single customer-edge device and physical connection on a provider-edge device. To accomplish this, Multi-VRF extends a limited amount of the provider-edge routing intelligence and functionality down to the customer-edge device for use in establishing secure, scalable VPNs on this device. This added functionality enables the customer-edge router device to support multiple VPN customers, each with their own unique VRF route table, on a single customer edge. For service providers, Multi-VRF reduces costly VPN-associated port burden on the provider-edge devices by allowing customer-specific VRF routing tables to be stored on a single device, maintaining the privacy and security of each customer's VPN connection and making the overall solution more cost-effective and ideal for deployment in VPN-dense areas.

VRF-Lite (also referred to as Multi-VRF-CE) is a recently developed version of Multi-VRF optimized for use on Cisco Catalyst access switching platforms. This new implementation allows compact, low-cost Cisco Catalyst customer-edge devices to support multiple VPN customers while only requiring a single physical uplink to the provider-edge device. The cost savings associated with the reduced customer-edge platform cost and provider-edge uplink port requirements can increase provider VPN profit margins while also increasing overall network scalability and capacity for VPN sessions. VRF-Lite is supported on Cisco Catalyst 3550 and Cisco 7600 series platforms.

Conclusion

The demand for high-speed metro Ethernet services is growing. Enterprise customers need metro connectivity solutions, which will allow them to reach beyond the bandwidth limits of T1/E1. Small businesses and residential customers are demanding the delivery of high-quality, bundled voice, video, and data services. Service providers require cost-effective solutions that address these needs and enable them to satisfy customers with a host of profitable services. The answer is metro Ethernet.

Metro Ethernet solutions make the most of high-bandwidth capabilities and low port cost to create highly resilient, multiservice network infrastructures. Metro Ethernet is the ideal medium for delivering reliable high-speed media and bandwidth services.

Metro service providers require flexible and innovative network infrastructure solutions built from equally flexible and innovative products. Cisco Metro Ethernet solutions provide the necessary balance of features and technologies to enable service providers to deploy leading-edge, cost-effective metro services to their customers.

When it comes to metro Ethernet, Cisco offers the unparalleled solution.

For more information about Cisco Metro Ethernet Solutions, contact your Cisco account manager today, or visit:

<http://www.cisco.com/go/metro>



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0208R) LW3663 10/02