

# Designing Tomorrow's Ethernet-Based MANs

---

## Executive Summary

*As the demand for inter-site bandwidth increases, businesses and government agencies are taking advantage of the high-speed Ethernet technologies already deployed within their buildings to communicate between their buildings. Ethernet is an easy-to-use, fairly inexpensive protocol with standard speeds, which makes it practically "plug and play." To extend communications beyond the office to multiple locations, Ethernet-based Metropolitan Area Networks (MANs) have filled that gap and have become very popular.*

*Careful consideration of the various Ethernet MAN designs, as well as engineering of the equipment used to connect the MAN to your network, is critical to meet current and future business demands. Failing to engineer both elements (equipment and network transport) could prevent your company from fully utilizing your network, and could dramatically affect your network applications. This paper will discuss important issues that need to be evaluated when designing your Ethernet MAN.*



### What is a Metropolitan Area Network?

A Metropolitan Area Network (MAN) is leased network connectivity interconnecting users and computers in a geographical area roughly equivalent to an extended large metropolis. MANs predominantly provide high-speed transport using Ethernet technology. Among the most popular speeds are: 10, 50, 100, 500 and 1,000 Mbps service speeds. Higher speeds, such as 10 Gbps MAN service, are becoming more available.

Ethernet-based MANs are high-speed networks confined to a moderately sized area (such as a large metropolis) using Ethernet as the transport protocol. Ethernet-based MAN networks offer two basic switching architectures:

- Point-to-point
- Multi-point

A point-to-point MAN connection facilitates communication between two sites (like a point-to-point circuit). Multiple point-to-point connections can be provisioned (multiplexed) to ride a single physical connection using Ethernet 802.1Q VLAN tagging. Each VLAN is mapped to a different point-to-point connection and has a committed information rate (CIR) value. CIR is the contracted amount of bandwidth transmitted over a connection. Packets exceeding the CIR may be rate-limited (discarded) by the service provider.

Multi-point MAN networks offer any-to-any communications among three or more sites, using Ethernet switching. Ethernet switching will forward multicast, broadcast and some unicast packets to all sites. That might be a concern and may require engineering considerations for large multi-point networks, but could be advantageous for smaller networks.

Ethernet makes MANs connections simple because customers can connect to the network through either a router or a switch. Layer-2 MAN service providers use Ethernet switching technology to switch customer packets between sites, and Multi-protocol Label Switching (MPLS) is often used to provide transport services to multiple customers while keeping customer traffic separate from each other. MPLS allows service providers to have customers share a very high-speed optical backbone rather than dedicating individual (slower speed) backbone circuits to individual customers, making the services more cost-effective.

Important differences exist between layer-2- and layer-3-based networks. These differences extend into MPLS networks that support both layer-2 switched Ethernet and layer-3 VPN services. The root of those differences is the protocol used to switch the traffic in the service provider network. Layer-2 MPLS uses Ethernet media access control (MAC) addresses and allows the user to manage routing tables and layer-3 MPLS uses IP addresses and routing is taken care of in the network.

In nearly all cases, a router or layer-3 switch should be used to connect an Ethernet MAN to a customer site. The type and size of layer-3 switch or router depends on the MAN architecture and speed of the MAN circuits. The following engineering characteristics should also be examined when choosing a router or layer-3 switch for a MAN connection:

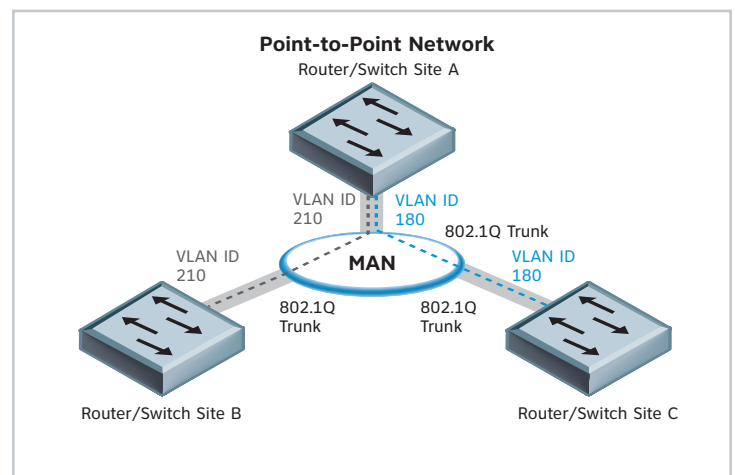
- Traffic shaping
- QoS capabilities
- Performance

OPT-E-MAN® service is a leading MAN service offered by AT&T. It offers connections across the metro area spanning a few or several hundred miles, depending on the size of the market area. Telecommunications companies generally offer MANs at very competitive rates compared with traditional circuits at similar speeds. OPT-E-WAN<sup>SM</sup> works like OPT-E-MAN® to extend Metro networks to Wide Area Networks.

### Common Network Architectures

#### Point-to-Point and Multi-point Networks

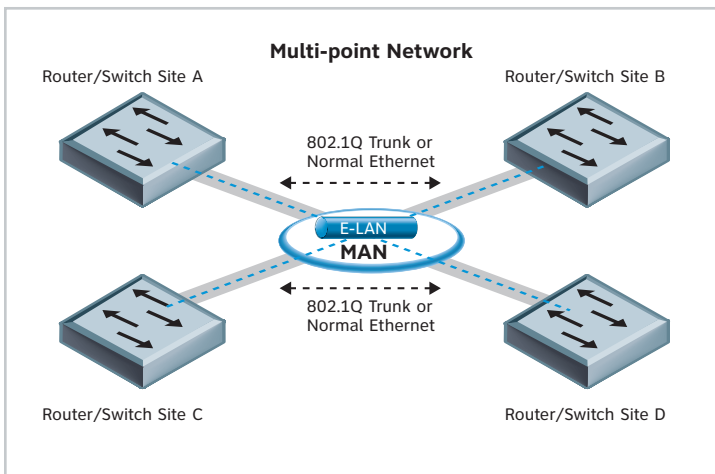
Many Ethernet services offer both point-to-point and multi-point services. Point-to-point service offers Ethernet communications between two sites. A single MAN circuit can support multiple point-to-point connections using a separate VLAN within an 802.1Q trunk. A different tagged VLAN is used for each point-to-point connection.



This concept is analogous to separate DLCIs within a Frame Relay circuit. In the above example, VLAN 210 provides communications between sites A to B and VLAN 180 provides communications between sites A and C. If site B wants to communicate to site C, the network needs to be engineered to first transmit the packet to site A via VLAN 210, then to site C via VLAN 180. In most cases, the service

provider and customer will assign a service rate or CIR to each VLAN path. The maximum number of site VLANs supported on a single MAN Ethernet trunk is generally dependent on the size of the trunk compared to the sum of the service speeds (CIRs) for the individual VLAN channels on that trunk (i.e., oversubscribing an 802.1Q trunk is not recommended).

Multi-point service provides any-site to any-site communication using virtual Ethernet bridging in the MAN cloud. The network will switch packets between all of the participating sites, using the destination Ethernet MAC address. As such, Ethernet broadcasts, multicasts and frames containing MAC addresses with unknown destination addresses will be flooded to every other site.



Each site connects to the MAN, using a single VLAN or traditional Ethernet connection. If VLANs are used over an 802.1Q trunk, it is possible for the multi-point connection to share a circuit with other point-to-point or multi-point connection services (which is fairly rare).

The service speed or CIR for each site need not be identical in a multi-point MAN network. It is also normal to oversubscribe the E-LAN – a site's CIR is often less than the sum of the other sites' CIRs. Often a site's CIR matches its MAN circuit speed in many multi-point networks (e.g., Gigabit CIR service over a Gigabit Ethernet interface).

## Common MAN Requirements

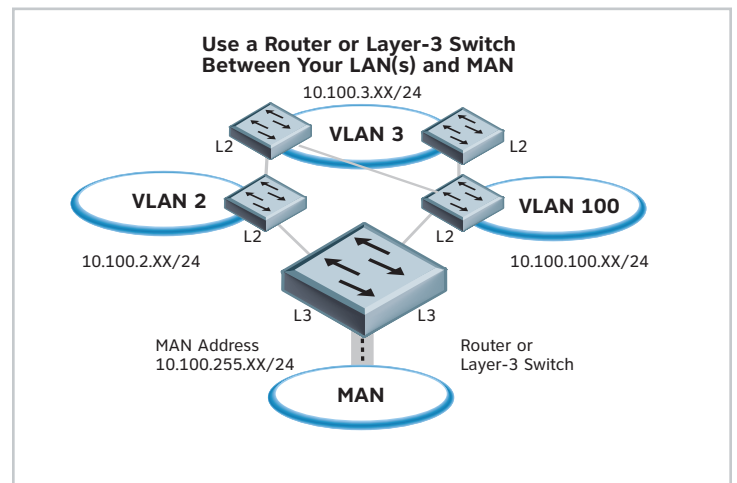
### MAC Address Limitations

It is important to remember that MANs operate on Ethernet (layer 2), not IP (layer 3) boundaries. Consequently, service providers and customers want to limit the number of MAC addresses associated with each MAN connection. A layer-3 switch or router accomplishes this by separating user VLAN(s) from the MAN VLAN(s). Only the MAC address of the customer's router or layer-3 switch will be transmitted over the MAN. This strategy:

- Eliminates unneeded MAN bandwidth consumption
- Increases network management capabilities
- Simplifies troubleshooting tasks
- May be leveraged to apply the customer's security policy
- Is considered "best practices"
- Reduces service providers MAC address tables

A router or layer-3 switch blocks traffic that needs not or should not be transmitted over the MAN.

When used in an IP network, the IP address assigned to the MAN connection will not be in the same subnet as the site's computers and servers. The diagram below exemplifies that.



Any router or layer-3 switch will effectively limit MAC addresses on the MAN, as well as meet industry best routing practices. The use of a router or layer-3 switch is highly recommended in MAN environments.

### Traffic Shaping

Ethernet interfaces come in fixed speeds of 10 Mbps, 100 Mbps, 1 Gbps and 10 Gbps. However, Ethernet MAN service typically offers CIR ranges from 1 Mbps to 1 Gbps (AT&T's OPT-E-MAN® CIR offerings are: 2, 4, 5, 8, 10, 20, 50, 100, 150, 250, 500 and 600 Mbps, as well as 1 Gbps). MAN providers will generally require a physical circuit that has sufficient bandwidth to carry the CIR for all of the virtual connections on it. Therefore, the sum of the CIRs must be ≤ to the Ethernet circuit speed (as depicted in the below chart).

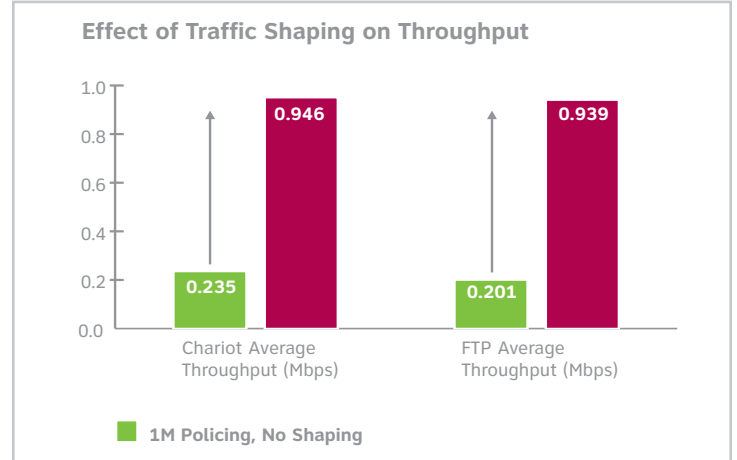
Σ CIR on Circuit	Circuit Speed
1 – 10 Gbps	10 Gig Ethernet
100 – 1,000 Mbps	1 Gig Ethernet
10 – 100 Mbps	100 Meg Ethernet
2 – 10 Mbps	10 Meg Ethernet

What happens if a customer purchases 250 Mbps service for a single point-to-point connection? Based on the above chart, a single connection with a CIR of 250 Mbps will be carried on a 1 Gig Ethernet connection.

Most service providers will rate-limit traffic entering the MAN to the CIR for each logical VLAN connection. Packets exceeding that rate will typically be discarded randomly. Those discards will often prevent effective TCP synchronization and can significantly disrupt networked applications. Thus, it is preferable to control the bandwidth being transmitted into the MAN using traffic shaping. In the above example, the 250 Mbps CIR connection on the 1 Gbps interface should be traffic shaped to 250 Mbps.

Engineering traffic shaping on the layer-3 switch or router's MAN interface solves the issues caused by rate limiting (including TCP synchronization) by having the router or switch temporarily buffer packets exceeding the VLAN's CIR until the resulting packet rate is within CIR limits. Traffic shaping is typically needed for each VLAN supporting a logical connection. Traffic shaping is not needed if the MAN circuit only supports a single VLAN that is assigned a CIR equal to the circuit speed (e.g., a 100 Meg Ethernet connection carrying a single VLAN with a 100 Meg CIR does not need traffic shaping).

AT&T Engineering tested the potential impact of traffic shaping. In the test results depicted below, the effective throughput without traffic shaping enabled was about 22%. Enabling traffic shaping greatly improved the effective throughput to 94%.



We also noticed that applications took five times longer to complete in a network without traffic shaping.

The traffic-shaping capabilities of the equipment a customer selects for each site's layer-3 switch or router should be considered when selecting a switch or router. If a site has multiple virtual MAN connections (common at a head-end office in a point-to-point network), traffic shaping may need to be applied independently to each VLAN connection.

In general, routers provide a richer and wider range of traffic-shaping capabilities, while switches provide wire-rate traffic shaping often at the expense of features and capabilities. Some switches offer no traffic-shaping capabilities, others offer port-based traffic shaping, and others offer traffic shaping for a limited number of VLANs. Traffic shaping on a router also requires carefully matching the router's performance characteristic with the MAN bandwidth requirements.

### Quality of Service (QoS)

If your network supports voice or other applications needing controlled latency and/or packet drops, the router or layer-3 switch selected for each site must support QoS. While QoS should be deployed throughout your network, it is very important to enable QoS on the MAN interface(s). If QoS is needed in your network, traffic shaping is critical – no effective QoS can be performed if packets have the potential to be rate limited in the MAN.

In general, the QoS strategy is to hold back packets that exceed the VLAN's CIR and transmit priority packets first when the high-priority packet can be transmitted without exceeding the CIR value. Lower-priority packets are transmitted after the high-priority packet, but still within the VLAN's CIR.

Full QoS control is possible on a point-to-point MAN network because the egress and ingress bandwidth for each site can be controlled. Traditional differentiated services (DiffServ) QoS are usually used for packet prioritization. DiffServ is the QoS strategy used in nearly all QoS-enabled networks today.

If a multi-point MAN network is deployed, a DiffServ prioritization strategy can still be used; however, the multi-point nature of the network will allow a site to be overwhelmed with (high- or low-priority) traffic from other sites (i.e., it is possible for multiple other sites in the multi-point environment to "gang up" on a single site). Fortunately, some MANs

such as AT&T's OPT-E-MAN® do not currently rate-limit traffic flowing to a customer site, just traffic flowing from a customer site. The lack of ingress rate-limiting to a customer site softens, but does not eliminate, QoS challenges associated with multi-point MAN networks.

Resource reservation protocol (RSVP) is an Integrated Services (IntServ) QoS strategy that addresses challenges associated with a multi-point network. With RSVP, individual clients and servers signal their QoS needs. Routers and layer-3 switches view those QoS requests and will only grant the bandwidth request if sufficient bandwidth is available. In a multi-point environment, routers or layer-3 switches can reject an RSVP request that would surpass the bandwidth allocated to that QoS class (thus eliminating the capability for sites to "gang up" on a single site). However, RSVP's "Achilles' heel" is that very few applications have implemented RSVP in their products and without application support, RSVP cannot be implemented effectively. Furthermore, some routers and layer-3 switch manufacturers also do not yet offer RSVP services.

The below chart summarizes the effectiveness of the QoS strategies on Ethernet based MAN networks:

	Point-to-point	Multi-point
DiffServ QoS	Fully Effective	Partially Effective
IntServ QoS	Fully Effective	Fully Effective

Please contact your AT&T representative for more information about the appropriate routers and switches to be used in a MAN environment.

**Differences Between L2 and L3 MPLS Networks**

Both layer-2 and layer-3 MPLS networks are popular. There are differences between them that should be considered when designing your network. In general, those differences include:

	L2 MPLS Networks	L3 MPLS Networks
Transport Protocol	Ethernet	IP
Packet Fragmentation Support	Not supported	Supported
Supported Transmission Architectures	P2P and/or m-point	Generally always multi-point
Packet Path Selection	Based on destination Ethernet address	Based on destination IP address
Broadcast support	Ethernet multicast and broadcast transmitted	Limited to directed IP broadcasts. Some IP multicast support
Layer-3 adjacencies	P2P: 1 per site M-point: N*(N-1)/2	One per site – customer router to provider edge router
Head end Oversubscription	Not supported	Supported

A layer-3 MPLS-based network provides IP communications between customer sites that are usually separated by long distances (there are some L2 MPLS networks like AT&T OPT-E-WAN that are also designed for long-distance communications). IP is the protocol used in most L3 MPLS networks, while Ethernet is used in most L2 MPLS networks. As such, only IP traffic can be forwarded in an IP MPLS network, while L2 MPLS networks will transmit IP, IPX, AppleTalk and any other protocol carried over an Ethernet packet. IP supports packet fragmentation (making two or more packets from a single packet that is too large to be transported though a network segment). Ethernet-based networks do not do this automatically. In a L2 MPLS network, the router or layer-3 switch connecting the network to your site can be engineered to provide any needed fragmentation services; this is called Traffic Shaping. Without Traffic Shaping, packets that are too large to be transmitted over an Ethernet segment would be discarded.

L3 MPLS networks use a packet's IP address to route packets through the network; Ethernet destination MAC addresses are used on an L2 MPLS network. There is much significance to that difference; including more efficient routing capabilities using the higher-level address. IP will only switch packets toward their intended destinations while layer-2-based networks will sometimes unnecessarily forward packets to more sites than required. In L3 networking, the network automatically routes the packets and in L2 networks, the end user can control the routing with their own router, routing tables and switches.

L3 MPLS networks almost always provide multi-point services (any site can directly send traffic to any other site on the MPLS network). WAN service providers use BGP extensions (BGP-MP) to provide multi-point transport services without requiring each site's customer equipment to establish an L3 adjacency to every other site on the network. Rather each customer edge router will establish a single L3 adjacency to the associated site's provider edge router.

This is not the case for a multi-point L2 MPLS network. Each router on an L2 multi-point network must establish one L3 adjacency to every other router on the multi-point network. The number of adjacencies required in a multi-point L2 network is:

$$Adjacencies = \frac{N(N-1)}{2}$$

Where N is the number of sites on the multi-point network.

This is not a concern for L2 multi-point networks with a limited number of sites. A network with six sites will require 15 adjacencies, while a network with 12 sites (twice the previous example) will require 66 adjacencies (more than four times the previous example). A network with 35 sites requires 595 adjacencies.

Layer-2 MPLS multi-point networks scale but cannot scale as large as layer-3 MPLS networks, and are a better choice for smaller networks or for routing larger bandwidth connections within a hybrid layer 2, layer 3 network. Larger Layer 2 networks require careful routing protocol engineering (as well as the equipment on which it runs).

Extremely large layer-3 MPLS networks are easily supported. Since the routing all takes place within the network, routing tables are not an issue and multiple locations can be added at any time without consideration to the impact of the whole network.

The L2 adjacency scaling factor for a point-to-point layer-2 MPLS network is significantly better than multi-point. A single adjacency is formed for each VLAN based connection (adjacencies = N). In most cases, customers keep L2 point-to-point networks fairly small because of head-end MAN circuit costs (remember, the sum of the CIR values for all VLANs supported on a single interface cannot exceed the speed of the Interface). While per megabit cost of a MAN is often much less than a WAN, the MAN costs can add up if you have multiple high-speed Ethernet connections at the head end.

Bottom line – Consider layer-2 Ethernet on MPLS if you have approximately 50 or fewer sites, want to maintain control over your routing and want to keep the same Ethernet connections throughout your network. Consider layer-3 IP on MPLS if you have more than 50 locations, don't want to manage routing tables and traffic is IP-based.

In addition, consider a hybrid network of both services if you need the elements of each. Use the layer-2 network for your more secure, high-bandwidth mission-critical data that you can route and manage, and use the layer-3 networking for your day-to-day, IP-based traffic (Internet, VoIP, etc). Many customers combine both for a fully connected integrated network that can suit their needs and change as they need.

AT&T VPN (AVPN) and Private Network Transport (PNT) are AT&T's primary L3-based MPLS offerings. AT&T OPT-E-MAN® and OPT-E-WAN are AT&T's primary L2-based services that run across AT&T's MPLS infrastructure.

MANs are extremely effective at meeting customers' growing bandwidth requirements. However, the engineering of the MAN architecture and the equipment used to connect each site to the MAN is critical.

**For more information contact an AT&T Representative or visit [www.att.com/business](http://www.att.com/business).**

