



White Paper

Provider Backbone Bridges bring massive service scalability to Ethernet

Introduction

Ethernet dominates the LAN (Local Area Network) and has done so for many years; approximately 97 percent of Internet traffic originates or terminates on an Ethernet interface. Now Ethernet seems poised to take a leading role in metropolitan and wide area networks, as enterprise demand for Ethernet services is predicted to reach \$22.5 billion by 2009 (source: Infonetics Research, April 2006).

Ethernet services in the Wide Area Network (WAN) are attractive to enterprises for the following reasons:

- **Cost** – Due to wide usage of Ethernet as an interface in networking, Ethernet is more cost-effective than other WAN technologies.
- **Simplicity** – By offering transparent Layer 2 connectivity, the service provider does not get involved in the customer's Layer 3 network. This makes provisioning and maintenance simpler, helps reduce operational costs and offers the customer greater security.

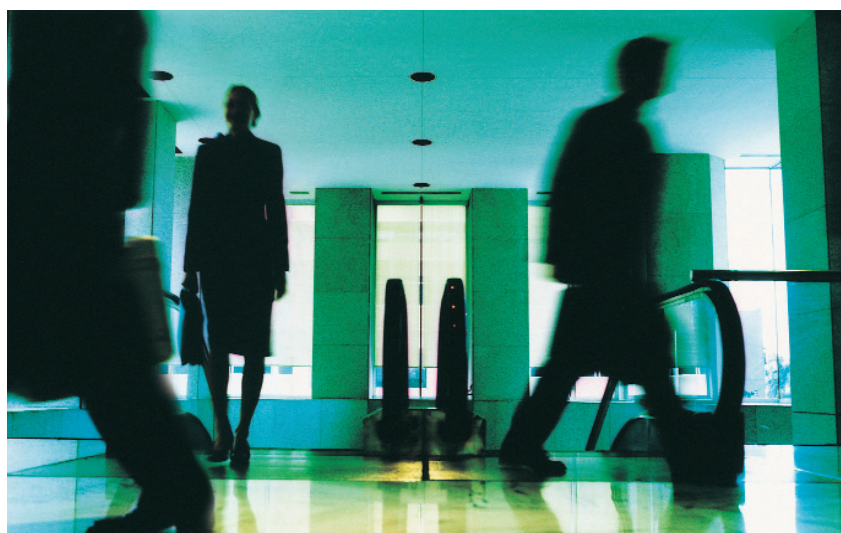
- **Flexibility** – Ethernet supports speeds up to 10 Gbps and bandwidth can be increased quickly and easily in increments of 1 Mbps, so enterprise users can match their bandwidth usage to their requirements.

As a result, Ethernet has evolved to support the demand for Ethernet services across the WAN, and emerged as Carrier Ethernet. Although initial Carrier Ethernet networks were built to support Ethernet services, many service providers are now using Carrier Ethernet networks as transport for backhaul of wireless and residential triple play traffic. In both these areas,

users' bandwidth demands are growing as video traffic is delivered to a variety of consumer devices and Carrier Ethernet offers the bandwidth required in a cost-effective manner.

Carrier-grade Ethernet services

Although customers are convinced of the advantages of Ethernet services, they are not willing to sacrifice the performance they've come to expect from their traditional WAN services. This means that the networks the service providers are building to deliver Ethernet services must be carrier-grade; in other words, they must meet the following criteria.



- **Scalability** – Enterprises need to be able to use Ethernet services over national and international distances, while service providers must support 100,000s of individual services.
- **Protection** – Traditional WAN services boast 99.999 percent availability, typically supported by 50 millisecond protection switching.
- **Quality of Service (QoS)** – Service providers must be able to offer a guaranteed end-to-end service level agreement (SLA), with Committed Information Rates (CIR) and Excess Information Rates (EIR).
- **Standardized services** – Must be offered to allow the seamless integration of TDM services, to support existing voice applications, and allow service providers to extend their geographic reach through interoperability agreements with competitors.
- **Service management** – TDM networks provide carrier-class Operations, Administration and Maintenance (OAM) that enables fast service activation and advanced trouble-shooting capabilities. Carrier Ethernet networks must match or improve on these capabilities.

These criteria have been incorporated into the Metro Ethernet Forum (MEF) Carrier Ethernet Certification Program. The MEF is the organization largely credited with transforming Ethernet, and this program facilitates the provision of consistent Ethernet services worldwide with products tested for their ability to deliver EPL (Ethernet Private Line), EVPL (Ethernet Virtual Private Line) and E-LAN services compliant with MEF technical specifications.

While the standard IEEE 802.3 Ethernet LAN protocol is still used, new service delivery technologies need to be added in order to create

Ethernet services. There follows an overview of the different Ethernet technologies used for service delivery over Ethernet networks.

IEEE 802.1Q Virtual LAN (VLAN)

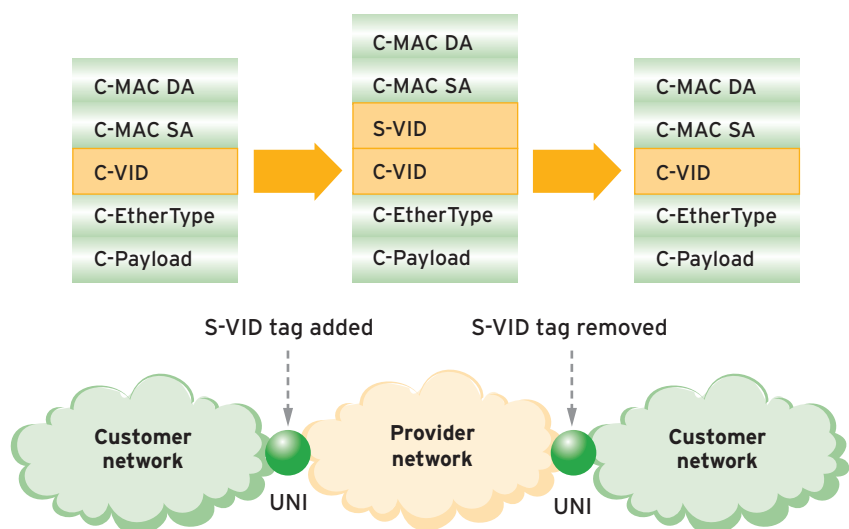
The basic technology standard used for delivering an E-LAN service is the IEEE 802.1Q standard for Virtual LANs (VLANs). This standard creates VLANs across a common LAN infrastructure to enable enterprises to support and separate traffic from different departments within a company (for example finance, legal and general administration). Each VLAN is identified by a Q-tag (also known as a VLAN tag or VLAN ID) that identifies a logical partitioning of the network to serve the different communities of interest.

IEEE 802.1Q works fine within the confines of a single organization, but is found wanting when service providers attempt to deliver Ethernet services to multiple end users over a shared network infrastructure. Issues arise because enterprises need to retain control over their own VLAN administration (such as assigning

Q-tags to VLANs), and over a shared infrastructure the service provider must control this to ensure that one customer's Q-tags do not overlap with another's. Also, because the Q-tag consists of a 12-bit tag, up to 4,094 possible service instances can be created. (Note: 4,096 service IDs are available, but two of these are reserved for administration.) Although this is sufficient for a LAN, it does not offer the scalability required to support Ethernet services in a large metropolitan area. What is needed is a method for defining secure Ethernet services to individual customers within which the customer can create further VLANs for departments or groups of users. There are two developing standards that support this approach: IEEE 802.1ad Provider Bridges (also known as Q-in-Q or VLAN stacking) and IEEE 802.1ah Provider Backbone Bridges (also known as MAC-in-MAC).

The standardization of these technologies is being driven by the IEEE 802.1 working group. The Provider Bridges standard was officially approved in December 2005, while Provider Backbone Bridges was

Figure 1. S-VID added to customer service frame



formally introduced as draft standard in March 2005 and it is expected to be officially approved in March 2007.

IEEE 802.1ad Provider Bridges (Q-in-Q)

Provider Bridges work by simply adding an additional service provider VLAN ID (S-VID) to the customer's Ethernet frame. This new S-VID tag is used to identify the service in the provider network while the customer's VLAN ID (C-VID) remains intact and is not altered by the service provider anywhere within the provider's network as shown in Figure 1. This solves the transparency problem experienced by IEEE 802.1Q.

As discussed, Provider Bridges use the S-VID to identify the service to which a customer's Ethernet frames are associated and therefore each service instance requires a separate S-VID. Because the S-VID consists of a 12-bit tag, Provider Bridges has the same scalability limitation of IEEE 802.1Q and only 4,094 services instances can be created.

In addition, Provider Bridges uses the same MAC address for the provider's and customers' networks. This makes

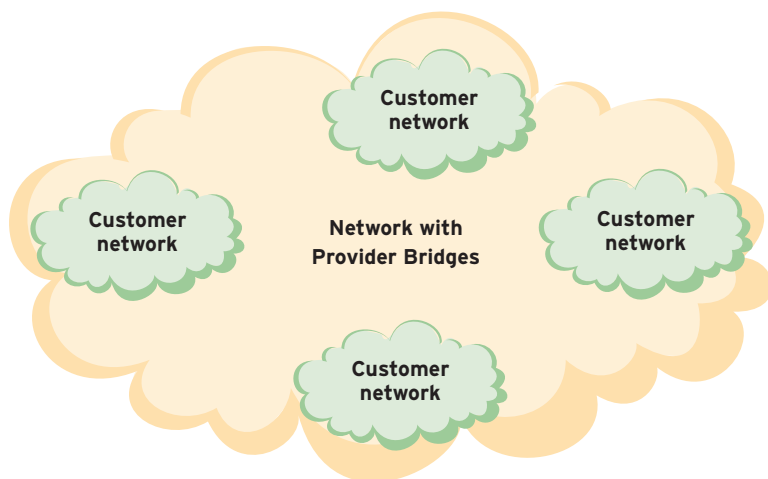
both networks appear as one large network to the provider's switches, as shown in Figure 2.

In the scenario depicted in Figure 2, the provider's and customers' MAC addresses are visible to all network elements and this creates a significant burden for core switches, as they must maintain a forwarding table for every MAC address in the service provider and customer networks. Also, any changes to the customer network will have an impact on the provider core. For example, when a new host is added in the customer's network, the new MAC address must be learned by the provider's switches. Or, when a failure occurs in the customer network, the resulting action taken by Spanning Tree Protocol (STP) can impact the provider network. These changes are outside the influence of the service provider, yet impact their network and create an unstable environment. From the customers' perspective, a potential security concern emerges from the fact that their addressing information is now visible outside of their secure network domain.

Provider Bridges does not provide separation between the provider and customer networks and this creates

problems where control protocols are concerned. Most Ethernet control protocols, such as Bridged Protocol Data Units (BPDUs) used by customer networks, must not interact with the provider's networking equipment. For example, STP used in the customer network must not interact with STP used in the provider network. BPDUs are identified by their destination MAC address and do not have a VLAN tag associated with them. For example, the Spanning Tree Protocol is identified by destination MAC address 01-80-C2-00-00-00. Provider Bridges cannot provide differentiation between customer and provider BPDUs because each entity's BPDUs have the same MAC address, and duplicate MAC addresses cannot be supported. This will cause unpredictable network behavior because the provider's networking equipment cannot distinguish between customer and provider BPDUs. The IEEE standard solves this limitation by introducing a different set of destination MAC addresses for BPDUs in the provider's network. However, to support these new provider BPDU MAC addresses, the provider must replace the existing Ethernet switches, because BPDU MAC addresses are not configurable. For this reason, Provider Bridges technology has significant limitations for E-LAN services that must support multiple customer control protocols.

Figure 2. Provider's and customers' MAC addresses visible to all networks

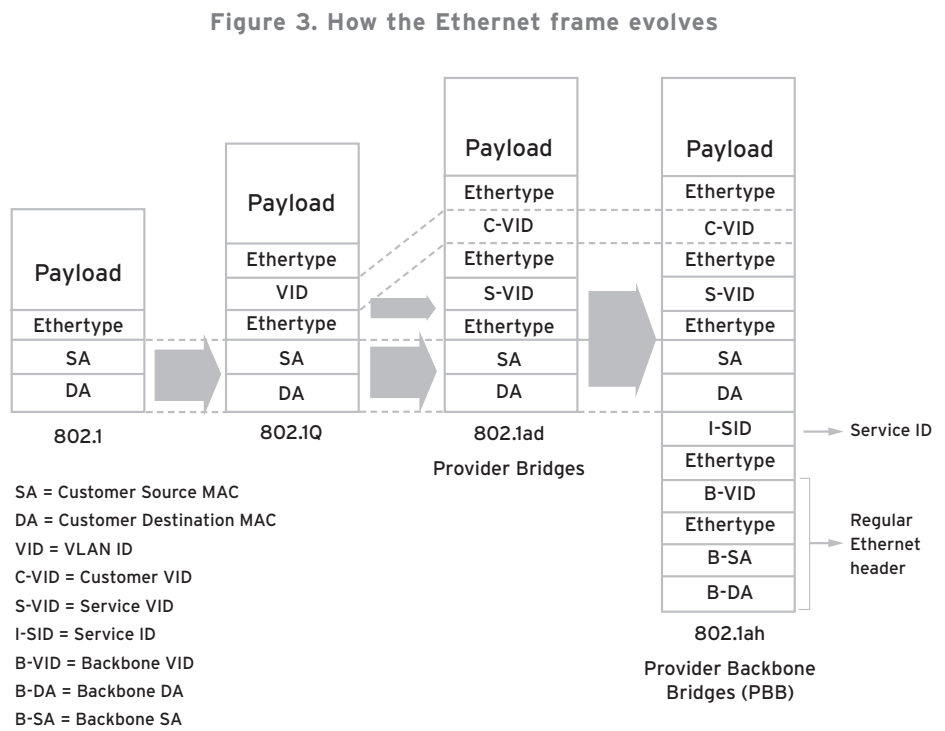


IEEE 802.1ah Provider Backbone Bridges (MAC-in-MAC)

Provider Backbone Bridges (IEEE 802.1ah) evolves the Ethernet frame by adding a MAC header dedicated to the service provider and, in doing so, adds a Backbone source and destination MAC address, a Backbone VLAN ID (B-VID) and a Backbone Service ID (I-SID) to the customer's Ethernet frame. Figure 3 illustrates the Provider Backbone Bridges frame and shows how this compares to the standard Ethernet frame (IEEE 802.1), Virtual LANs (IEEE 802.1Q) and Provider Bridges (IEEE 802.1ad).

The main benefit of Provider Backbone Bridges is that the 24-bit I-SID identifies the service in the provider's network. This means Provider Backbone Bridges provides up to 16 million services, completely removing the scalability problems of Provider Bridges.

In addition, Provider Backbone Bridges provides clear separation between the service provider and customer networks, because each has a dedicated set of MAC addresses as shown in Figure 4. When an Ethernet frame reaches the Ethernet UNI (User Network Interface), the service

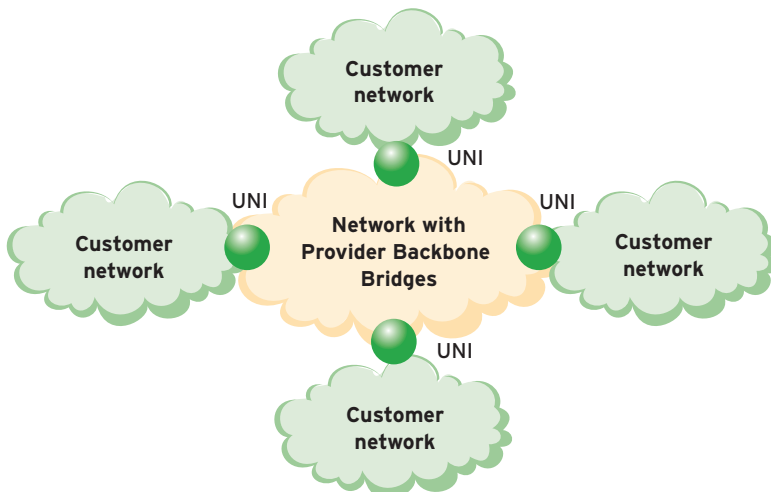


provider MAC address is added to the customer's Ethernet frame, and within the service provider network switches check this MAC address against their forwarding tables. This is an added advantage in that only switches at the edge of the provider network need to be Provider Backbone Bridges-enabled. Switches in the core of the network switch on a standard MAC header (in this case, the service provider header) and so any IEEE 802.1 Ethernet switch will suffice.

This solution allows customers' MAC addresses to overlap with the provider's MAC addresses, because the customers' Service Frames are tunnelled by Provider Backbone Bridges and are not used when switching frames inside the provider's network. As a result, customers are free to assign identifier and class of service values to their VLANs without concern that they will be altered by the service provider. Meanwhile, the service provider does not need to worry about coordinating VLAN administration with its customers.

Also, because the service provider's switches only use the provider MAC header, there is no need for them to maintain visibility of customers' MAC addresses, reducing the burden on the forwarding tables in the provider's network. This also ensures that changes to the customers' networks do not impact the provider network, improving the stability of the service provider's network. Finally, customer security is improved, because the service provider switches are no longer inspecting the customer MAC header.

Figure 4. Provider/customer MAC address separation at the UNI



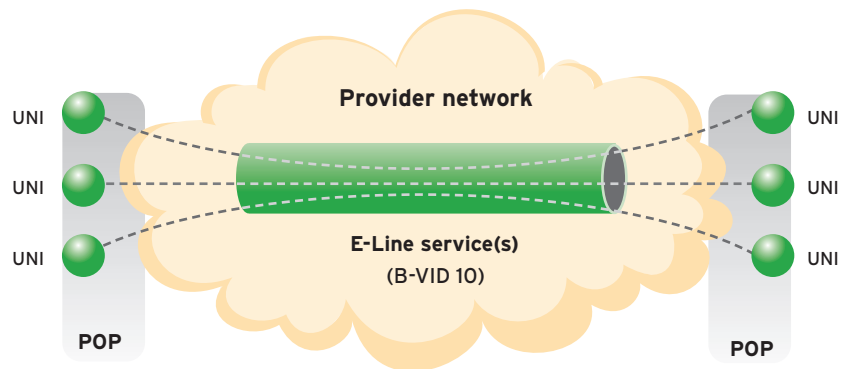
Another benefit of Provider Backbone Bridges is that because the I-SID is used for service identification, the Backbone VLAN ID (B-VID) can be used to segregate the service provider's network into regions or "zones" to simplify traffic engineering. Backbone VLANs enable the support of multiple customer services instances; for example, a B-VID can be engineered to support 1,000 10 Mbps E-Line services between POPs, as in Figure 5.

This means the service provider engineers the network once when the B-VID is set up. Individual services can then be activated at the source and destination nodes and supported over the B-VID up to its engineered limits. With Provider Bridges, each individual service needs to be configured across the network node-by-node, creating a substantial operational burden.

Since Provider Backbone Bridges tunnels customers' Service Frames, all customer Ethernet Control Protocols (BPDUs) are tunneled transparently across the provider's network. This allows Ethernet Control Protocols to be used independently by the customers' networks and the provider's network. As discussed, Spanning Tree Protocol (STP) in the customers' networks must not interact with STP used in the provider's network. STP is identified by its destination MAC address 01-80-C2-00-00-00 and with Provider Backbone Bridges, the customers' STP BPDUs are tunneled through the provider's network. Therefore, both the provider and customers can simultaneously use the standard STP destination MAC address with no additional provisioning required on the provider's switches.

This allows the provider to use the standard BPDUs MAC addresses on the existing switches in the network.

Figure 5. Single P-VLAN for multiple service instances



Summary

Ethernet services have emerged as an attractive proposition because they offer more cost-effective bandwidth than traditional WAN services. This has led to a requirement for Carrier Ethernet networks that can deliver the benefits of Ethernet services, with the carrier-grade performance of traditional WAN technologies.

In an effort to deliver carrier-grade Ethernet services, two emerging standards are evolving from the original IEEE 802.1Q VLAN standard: IEEE 802.1ad Provider Bridges (Q-in-Q) and IEEE 802.1ah Provider Backbone Bridges (MAC-in-MAC).

Provider Bridges adds an additional service provider VLAN ID (S-VID) to the customer's IEEE 802.1Q tagged frame. This technique is sometimes known as VLAN stacking. Service providers can now offer Ethernet services that are uniquely identified by an S-VID over a Carrier Ethernet network. Customer VLANs can be transparently mapped to these S-VIDs, giving the customer peace of mind that their internal VLANs will not be altered in any way by the service provider.

Provider Backbone Bridges builds on this concept by adding a service provider MAC header in front of the

customer MAC header. The overall network is now treated as separate service provider and customer domains. In the service provider domain, the network switches on the service provider MAC header and the customer MAC is not visible. This introduces strict demarcation between the customer and service provider, enabling a truly hierarchical approach to the network. This approach brings the following benefits:

- **Scalability** – Ethernet services are identified by a service label in the service provider MAC header, allowing up to 16 million services to be identified. Provider Bridges can only support 4,094 services.
- **Lower capital expenditure** – The switches in the service provider portion of the network only need to learn the service provider MAC addresses (and not the customer addresses), thereby reducing the memory and processing power required and ultimately the cost of the Ethernet switches in the service provider's network.
- **Robustness** – The service provider's network is now more robust. It is isolated from broadcast storms and potential forwarding loops created in the end customers' networks.

- **Security** – Because there is a clear demarcation point between the customer and service provider networks, there is no requirement for either party to have any knowledge of each other's addressing scheme. This significantly increases the security of their network, services and applications.
 - **Simpler operations** – The service provider can plan their network without worrying about overlapping VLAN or MAC addresses with those of their customers creating conflict in its network.
 - **Traffic engineering** – Provider Backbone Bridges allows Backbone VLANs to be configured, so that each support multiple Ethernet services. This simplifies service activation, as new services can be added to an existing Backbone VLAN without the need to configure each individual service across the network.
 - **Transparency** – Ethernet Control Protocols can be tunneled transparently, ensuring that customer and service provider networks operate independently.
- Finally, because service provider switches in Provider Backbone Bridges networks use a standard MAC header to forward frames through the network, standard Ethernet switches can be used in the core of the network. Only at the network edge are Provider Backbone Bridges-enabled devices needed to encapsulate customer frames in the service provider MAC header. This means Provider Backbone Bridges capabilities can be introduced gracefully to existing Carrier Ethernet access and aggregation networks.

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

For more information, contact your Nortel representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

Nortel, the Nortel logo, Nortel Business Made Simple and the Globemark are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2007 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel assumes no responsibility for any errors that may appear in this document.

In the United States:

Nortel
35 Davis Drive
Research Triangle Park, NC 27709 USA

In Canada:

Nortel
195 The West Mall
Toronto, Ontario M9C 5K1 Canada

In Caribbean and Latin America:

Nortel
1500 Concorde Terrace
Sunrise, FL 33323 USA

In Europe:

Nortel
Maidenhead Office Park, Westacott Way
Maidenhead Berkshire SL6 3QH UK

In Asia:

Nortel
United Square
101 Thomson Road
Singapore 307591
Phone: (65) 6287 2877



> BUSINESS MADE SIMPLE