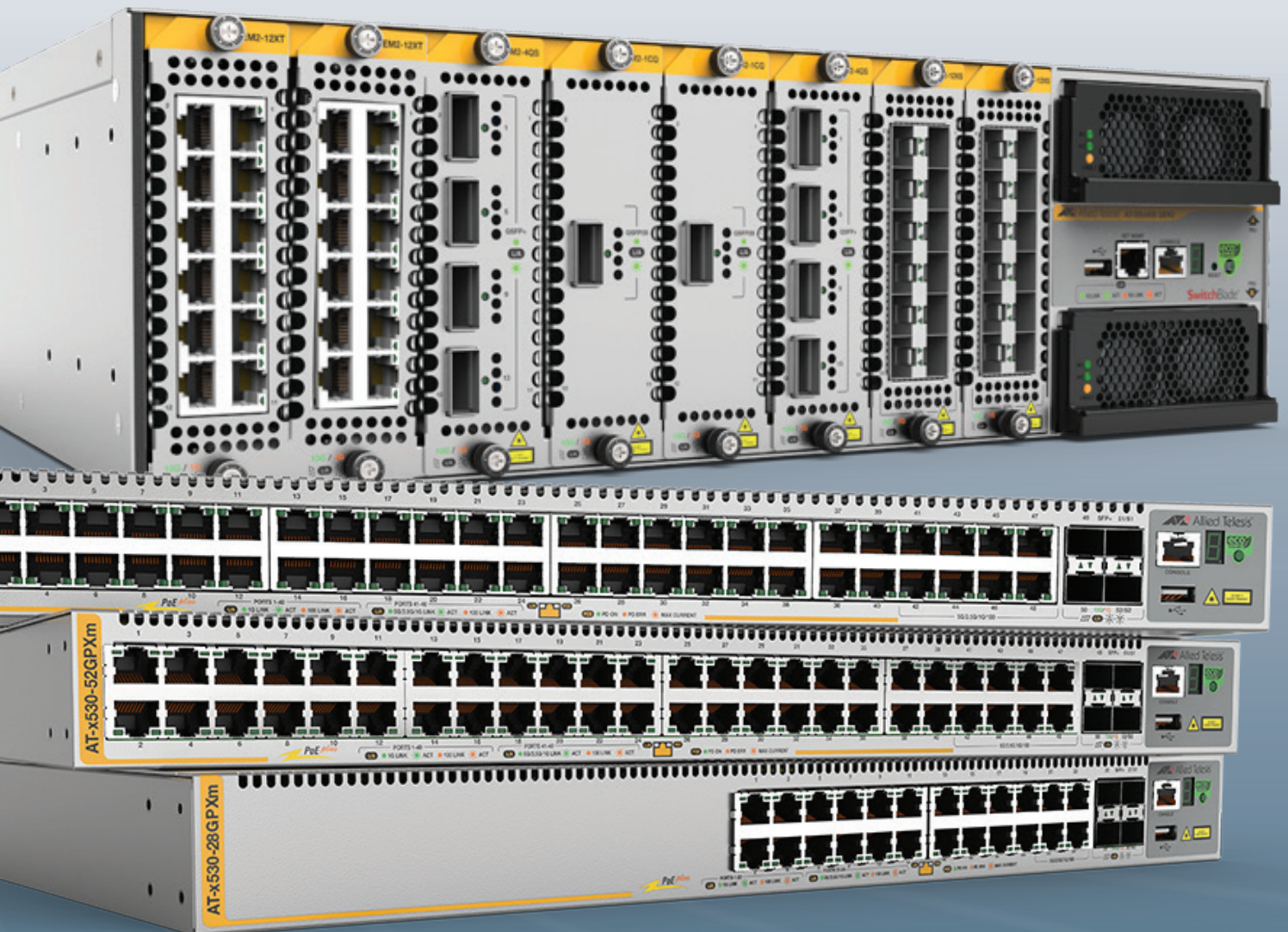Allied Telesis™

Ethernet-based Network Virtualization for the Enterprise

NETWORK SMARTER

Introduction

The concept of Tunneling Layer 2 and Layer 3 connections across a shared Layer 2 network used to be the preserve of network service providers. These days however, it is also common for an Enterprise network to be based around this model. It provides an effective solution in any number of situations where an Enterprise network consists of semi-autonomous entities that need to share common central connectivity.

For example:

- connecting independent departments in a campus environment
- shared LAN services within a large hospital
- providing connectivity within an airport for airlines, retailers, regulatory agencies, and so on
- access to shared resources within a school district
- a municipal network connecting multiple local government agencies
- providing connectivity for tenants in an MTU or a retail mall

In all of these cases, the key requirement is to build a single central network that allows individual entities to overlay their own virtual networks over this shared infrastructure.

Invariably, the accompanying requirements are:

- Security: no data leakage between different Virtual Private Networks (VPNs)
- Resilience: rapid recovery in the event of link or node failure in the central network
- Flexibility: options to provide tunneling at Layer 2 or Layer 3
- Quality of service: low latency and very little traffic loss for real-time services
- Simplicity: easy to manage, and easy to troubleshoot

At present, there is no established name for this type of network infrastructure. This document will refer to it as a **Shared Layer 2 Backbone**.

Allied Telesis provides a robust, scalable Shared Layer 2 Backbone implementation that meets all of the requirements above, and more.

List of terms

Multiprotocol Label Switching (MPLS)
A mechanism that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

Shared Layer 2 Backbone
This document uses this term to refer to the concept of tunneling Layer 2 and Layer 3 connections over a shared Layer 2 network.

Virtual Routing and Forwarding (VRF)
This technology allows multiple routing domains to co-exist within the same device at the same time. Routing domains are independent, so overlapping IP addresses can be used without causing conflict. This enables multiple virtual IP networks to exist independently on the same physical network.

VLAN Double Tagging (Q-in-Q)
A process in which an ethernet switch appends an extra VLAN tag onto packets that it receives on certain ports. This enables multiple VLANs to be tunneled across a Layer 2 network, encapsulated within another VLAN.

Allied Telesis solution

Allied Telesis has long recognized that the future of the modern data network lies with IP over Ethernet.

The ability to support Layer 2 and Layer 3 VPNs using Allied Telesis equipment requires an infrastructure that utilizes the following 3 key technologies:

1. **Virtual Routing and Forwarding Lite (VRF-lite)**
   This is required to maintain separation between the different IP networks within the Shared Layer 2 Backbone

2. **Ethernet Protected Switching Ring (EPSR)**
   This provides path resiliency, with extremely rapid (50ms) recovery

3. **VLAN Double Tagging**
   This provides Layer 2 tunneling across the shared backbone

The example on the right illustrates an implementation of this:

VLAN Structure

The tenant's VLAN structure is encapsulated in a single QinQ VLAN for secure high speed access across their own 'virtual' network to other office space, the data center and Internet.
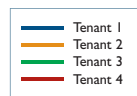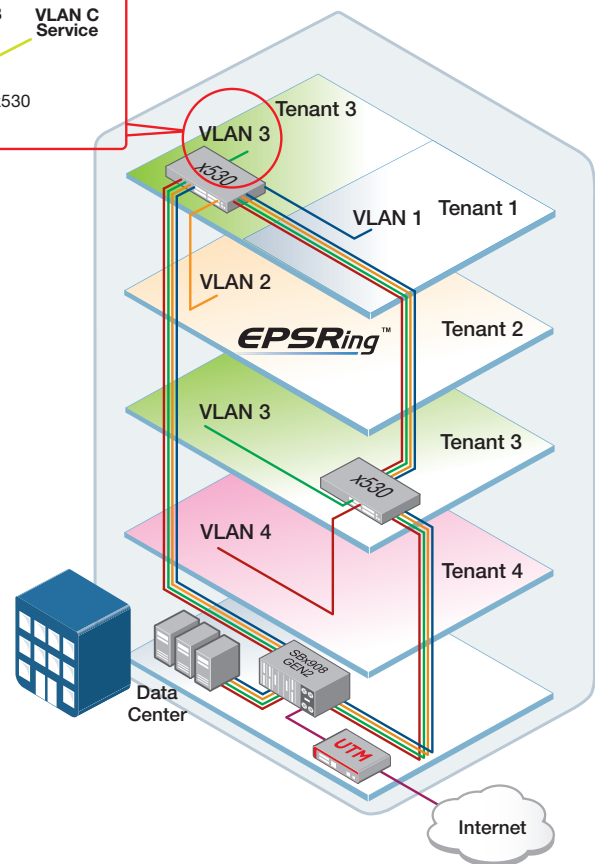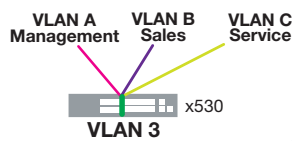
VLAN A Management
VLAN B Sales
VLAN C Service
x530
VLAN 3

VLAN 3 Tenant 3
VLAN 1 Tenant 1
VLAN 2 Tenant 2
EPSRing™
VLAN 3 Tenant 3
VLAN 4 Tenant 4
Data Center
Internet

Tenant 1
Tenant 2
Tenant 3
Tenant 4

Figure 1

How it works

This section examines in more detail how each of the 3 key technologies contributes to the solution.

1. VRF-Lite provides Layer 3 virtualisation
VRF-Lite enables completely separate IP networks to be overlaid on the same physical infrastructure.

The network's routers maintain separate routing tables for individual IP networks, and separate instances of routing protocols (OSPF, RIP or BGP) to populate the separate routing tables.

The IP networks, referred to as VRF instances, operate as completely functioning routing domains, with routes that are dynamically exchanged within each domain. However, the VRF-Lite functionality on the Allied Telesis Layer 3 switches ensures total separation between the different routing domains.

The following example shows Allied Telesis x930 Series switches performing VRF-lite, and thus acting as the Provider Edge (PE) switches in the Shared Layer 2 Backbone:

Virtual Network

Virtual Network #3
Virtual Network #2
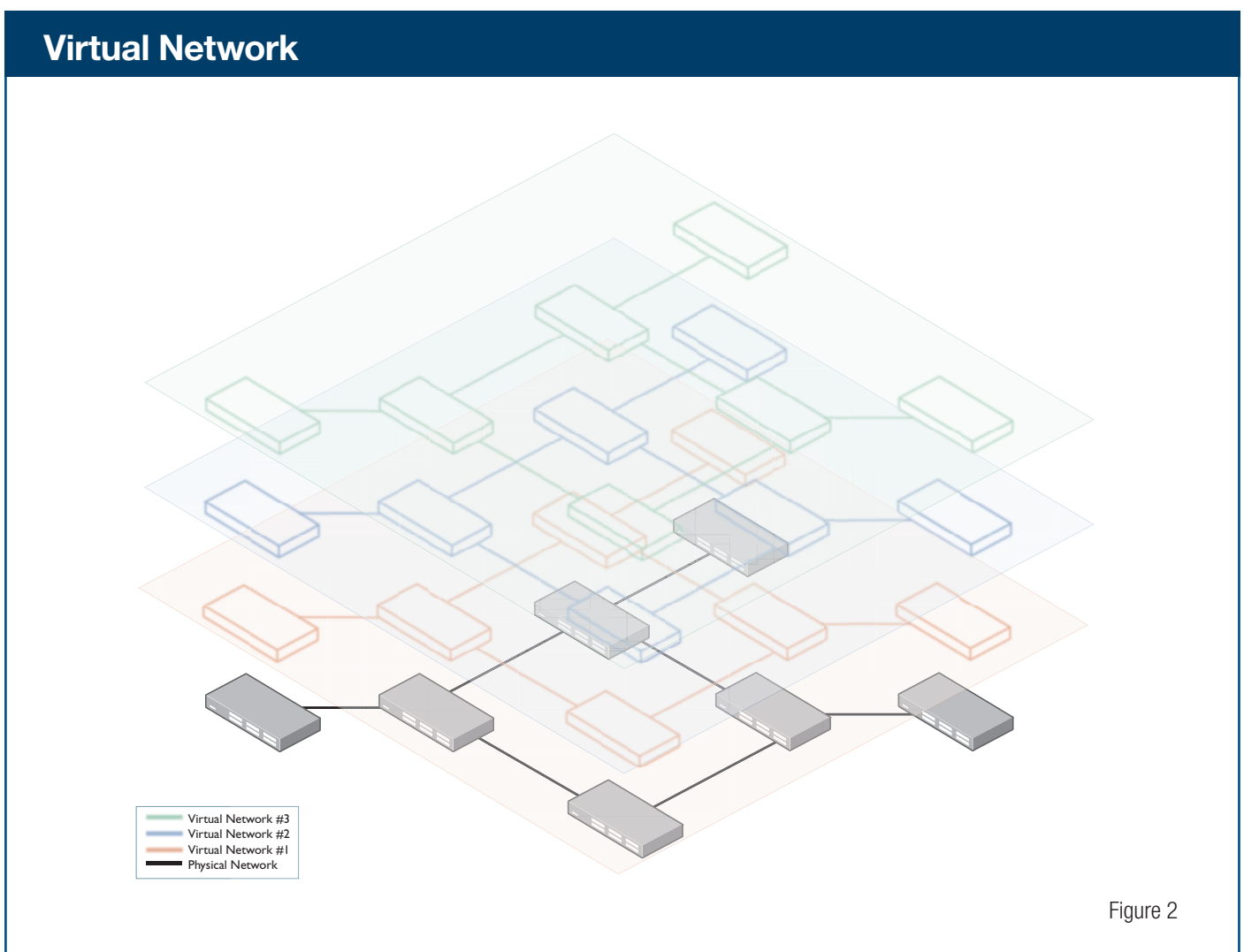Virtual Network #1
Physical Network

Figure 2

Different VRF instances are connected to different ports on the 'customer-facing' side of the switch. The VRF instances are each associated with a VLAN, so that on the 'provider' side of the switch, the VLAN tags on the packets indicate which VRF they are associated with. The following example illustrates this:
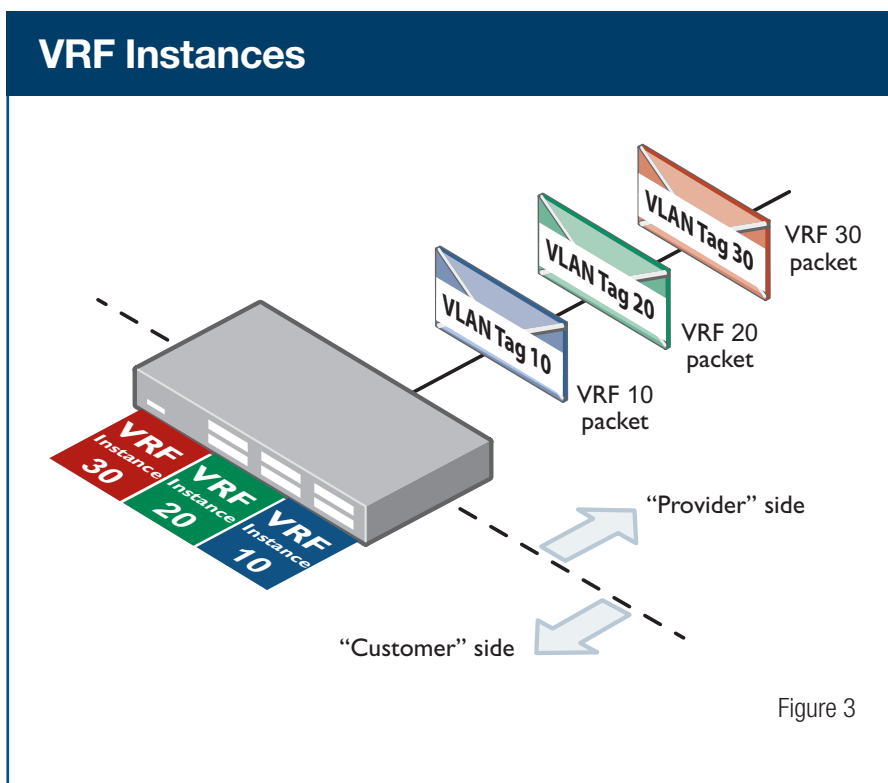
VRF Instances

Figure 3

Quality of Service (QoS) marking can be applied to the packets as they are Layer 3 switched within the VRF instances. Policies defined in the PE switches determine the Class of Service (CoS) values that are inserted into the packets' VLAN tags. The switches within the shared Layer 2 backbone then apply QoS (I.e. prioritization, policing, and shaping) based on these CoS values.

2. EPSR provides a resilient Layer 2 network

EPSR provides a highly responsive resilient Layer 2 network. Based on Ethernet rings, with EPSR your network can recover from lost nodes or links in 50ms or less. This provides the level of resilience required for real-time applications. A number of Allied Telesis switch series also support the standards-based G.8032 Ethernet Ring Protection protocol, which also provides high-speed failover.

Simple to set up, and with very little operational overhead, EPSR uses a simple Ethernet-based protocol to protect Layer 2 rings.

The EPSR-based backbone is very flexible:

■ There is no limit on the number of nodes in an EPSR ring.
■ The topology can consist of multiple rings, using EPSR superloop.
■ The links in a ring can be copper or fiber, and of any bandwidth.
■ Copper links and fiber links can exist in the same ring.
■ Links in the ring can be aggregated.
■ A variety of Allied Telesis products, stacked or unstacked, can be joined in an EPSR ring.

As well as being flexible in design, the backbone is simple to expand—you can add new nodes or more bandwidth with almost no service interruption. Data that is allocated per-VRF VLAN tag can be transported through this resilient backbone without any extra tagging or encapsulation.

The following diagram shows a pair of EPSR rings with VRF routers attached. The coloured paths show the routes that different VRFs use to traverse the EPSR rings.
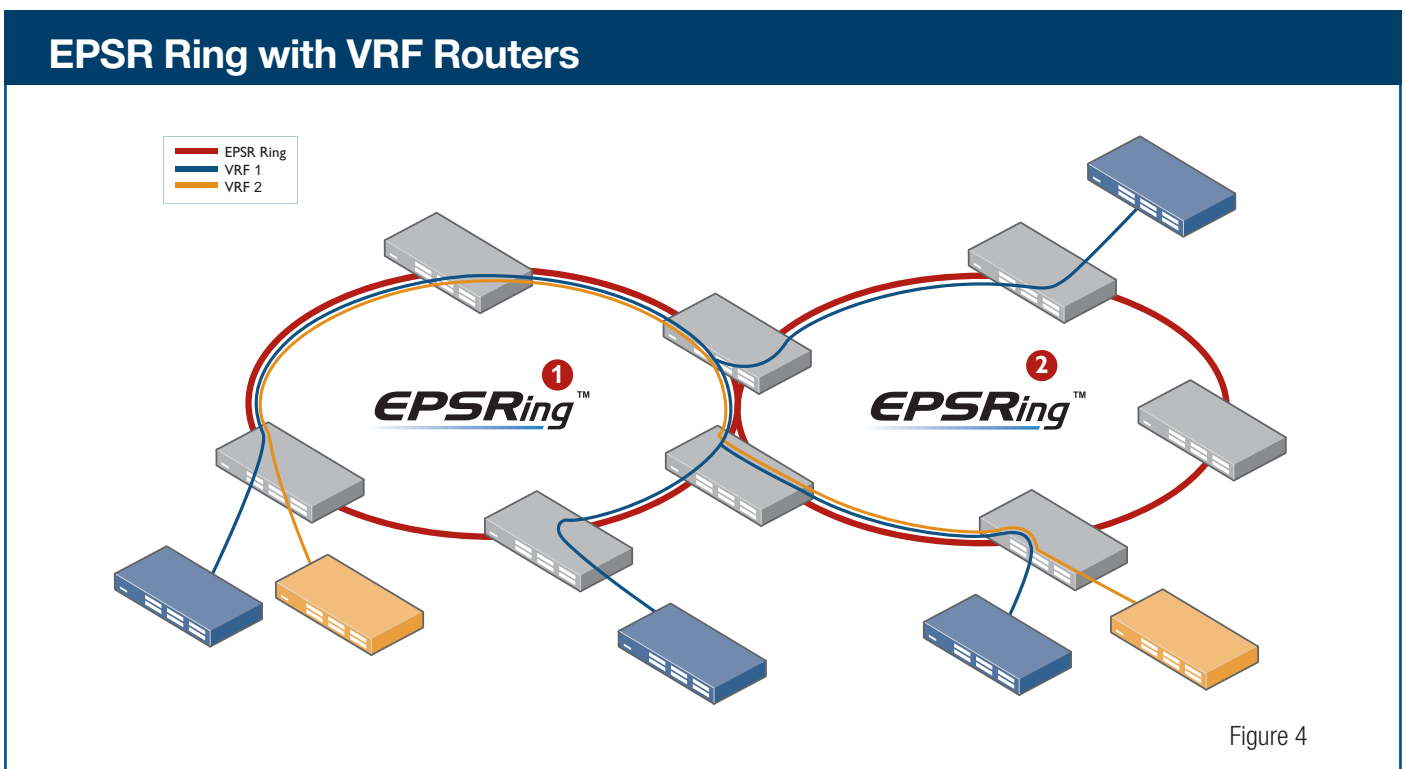

EPSR Ring with VRF Routers

Figure 4

3. Layer 2 tunneling with VLAN double tagging

Routing traffic across the shared backbone using L3 VPNs does not suit all situations—in some cases, it is preferable to simply tunnel VLANs directly across the backbone. The Allied Telesis solution supports this with VLAN double tagging (Q-in-Q). You can provision double tagging on a per-port basis, and it can be performed on the same Layer 3 switches that are providing VRF-lite routing.

The following diagram illustrates 3 switches that are connected to an EPSR ring. One switch is performing double tagging and VRF. Double-tagged traffic goes to one of the other switches, and the VRF traffic goes to the other.
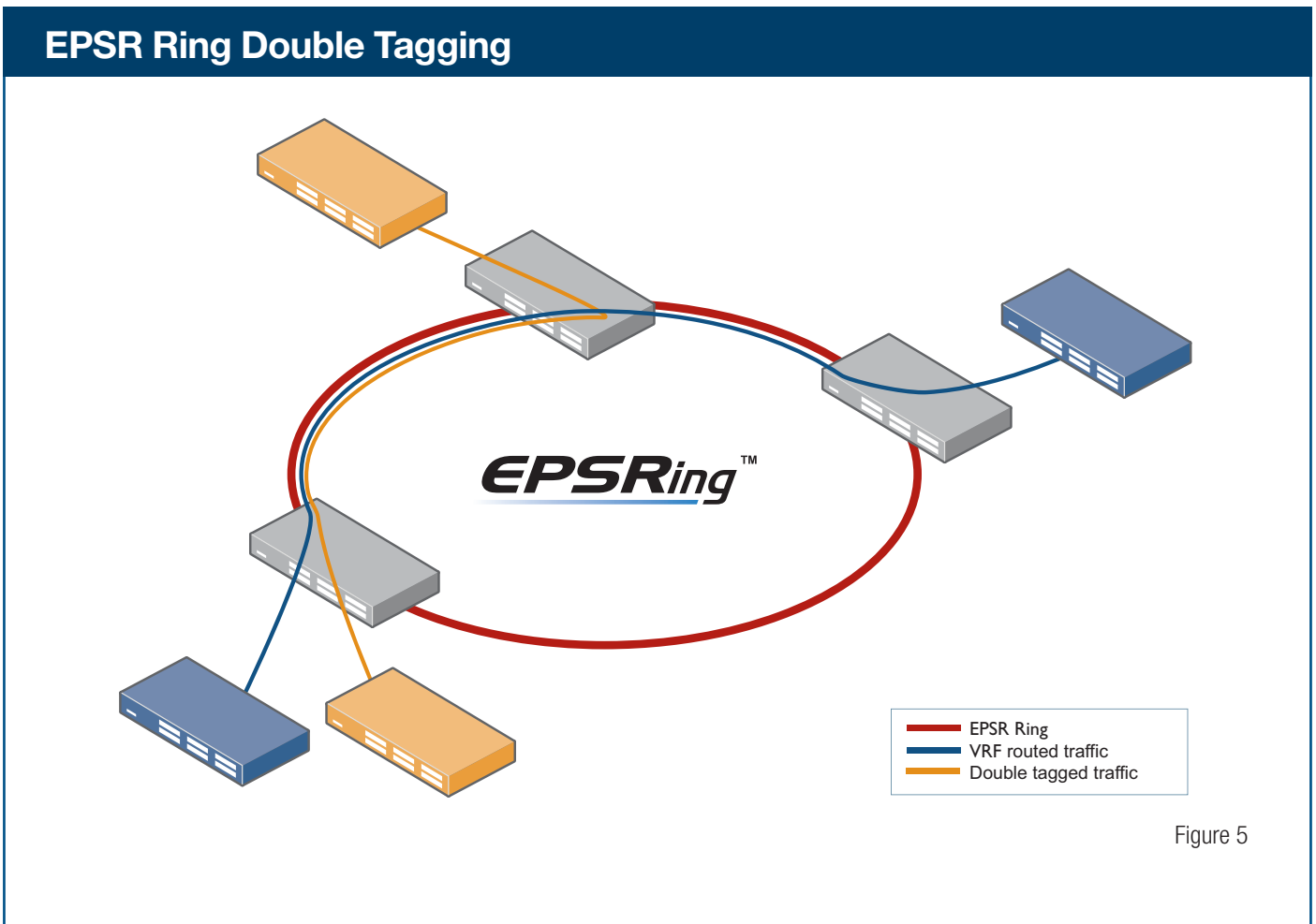
EPSR Ring Double Tagging

EPSRing™

EPSR Ring
VRF routed traffic
Double tagged traffic

Figure 5

Scalable design options

The x930 family of switches can themselves form the shared backbone, or they can provide a distribution layer that feeds into a Layer 2 backbone consisting of highly reliable components. For example, SwitchBlade x908 GEN2 stacks, or a SwitchBlade x8100 chassis.

The diagram to the right shows an EPSR ring of x930 switches with combined distribution and back bone layers:
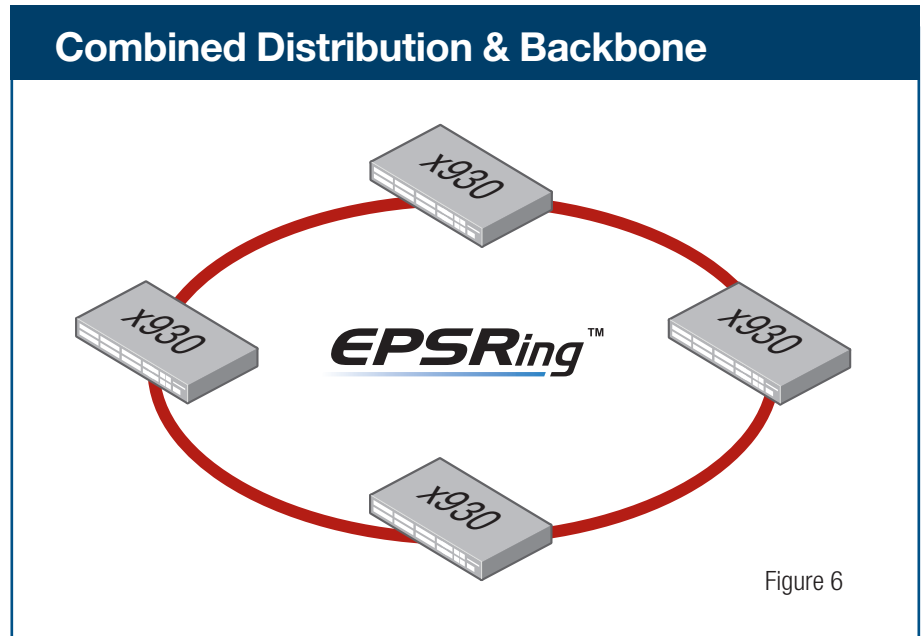
Combined Distribution & Backbone

Figure 6

The diagram below shows x530 switches connecting into an EPSR ring consisting of a SwitchBlade x908 GEN2 stack, a SwitchBlade x8100 chassis, and an x950 Series switch, with separate distribution and backbone layers:
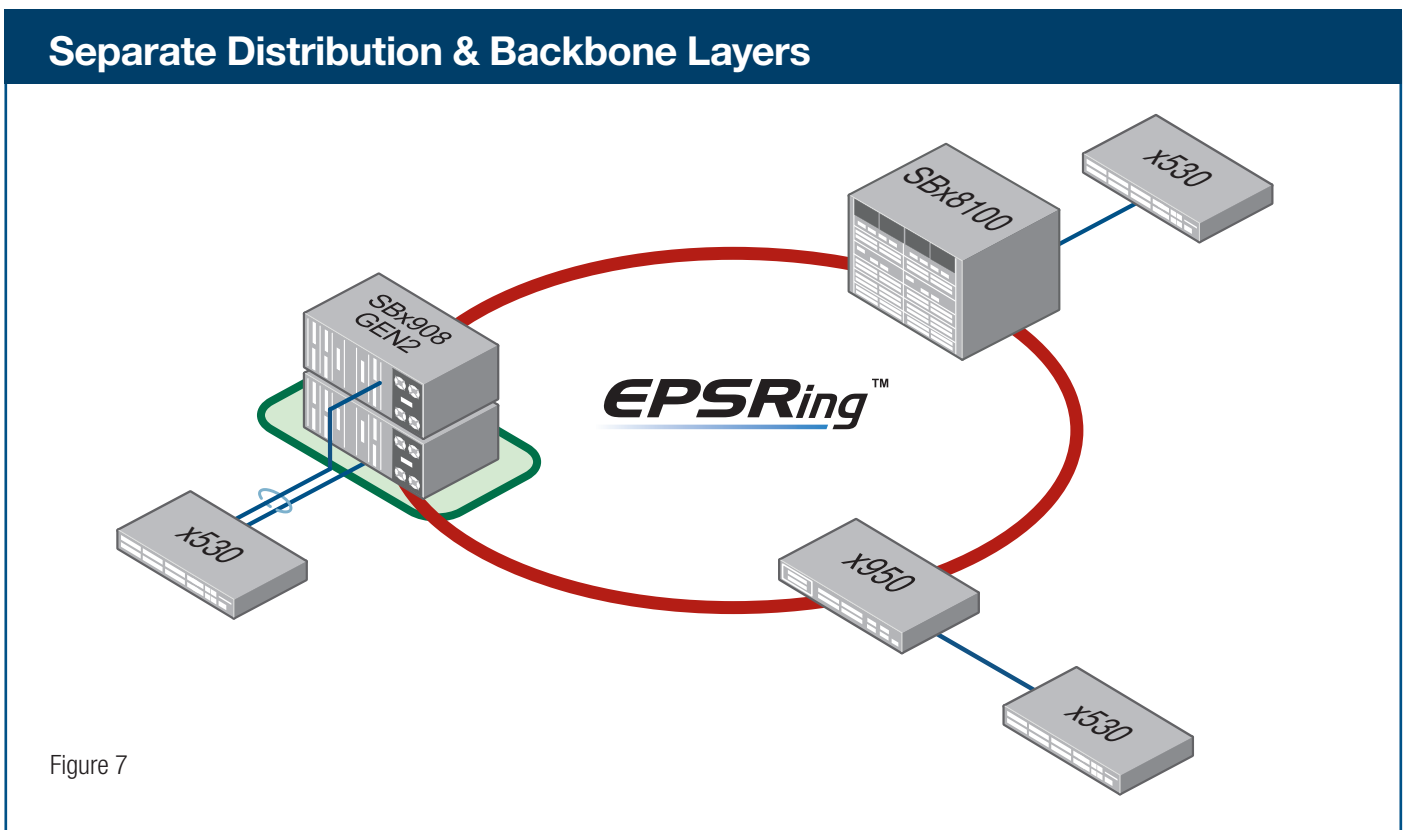
Separate Distribution & Backbone Layers

Figure 7

Comparison with MPLS

A number of enterprises have employed MPLS to implement their shared Layer 2 backbone. This section compares the Allied Telesis IP-over-Ethernet solution with an MPLS-based solution. It shows the claimed benefits of an MPLS-based solution, and considers whether or not it really does have an advantage over the IP-over-ethernet solution.

Table 1: MPLS claims and reponses

CLAIM MADE FOR MPLS SOLUTION	RESPONSE
Switching in the backbone is the most efficient, as it is based on just the MPLS label.	In a pure Ethernet backbone, switching is based only on VLAN tagging, which is equally as efficient.
MPLS hides IP addressing, so separate networks that use overlapping IP address ranges can share the same backbone switches.	The key enabling technology for the separation of IP domains is VRF. It is just as effective to use VLAN tagging to confine traffic into VRF instances as it is to use MPLS labels.
MPLS is a multi-protocol solution, so protocols other than IP can be transported across the backbone.	VLAN double-tagging is equally as multi-protocol as MPLS. The process of using a VLAN to encapsulate another VLAN for transportation across the backbone places no restriction on any higher-layer protocols being carried within the encapsulated VLAN.
MPLS sets up label paths automatically, without any need to statically configure the path.	Although the VLAN membership must be statically configured on backbone network ports, two points should be considered: 1. Configuring VLAN membership on ports is very simple, and can even be scripted. 2. In an Enterprise, the addition of a new entity in need of network separation is not a frequent event. So, in an Enterprise network, the total operational cost saving provided by MPLS's automatic path creation is very little.
MPLS provides QoS functionality.	Ethernet CoS marking enables QoS to be applied to different traffic types. In the end, the QoS marking scheme is not important. The important factors in QoS are: 1. the richness of the policy engines in the distribution switches, and 2. the power of the prioritization, policing and shaping features in the backbone switches. These factors are agnostic to which protocol is carrying the QoS marking in the packets.
MPLS can quickly re-route around broken links.	EPSR is an extremely effective mechanism for link recovery.

Advantages of an IP-over-Ethernet solution

There are many advantages of an IP-over-Ethernet solution. The Allied Telesis solution is simple, reliable and effective.

The major advantage is simplicity. Using MPLS in the backbone network adds an extra layer of complexity for no value. VLAN tagging is a simple and familiar technology. Given that mapping tunnels onto VLAN tags provides and effective solution, there is no need to employ another separate protocol for applying labels to tunneled traffic.

Static configuration of VLAN membership on backbone ports avoids the need to understand and troubleshoot any path establishment protocol. Backbone switch configuration can be kept very simple.

Additionally, using a pure IP-over-Ethernet solution lets you avoid being locked into having to use MPLS-capable equipment. Removing unnecessary elements from the solution, and keeping with more universal technologies broadens the range of options for equipment to use in the shared network.

About Allied Telesis

For more than 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Autonomous Management Framework™ (AMF) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and "things"—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at **alliedtelesis**.com

Allied Telesis™