White Paper

VLAN Best Practices

A VLAN is a logical grouping of two or more devices. This logical grouping may extend across many switches. The devices are grouped based on a number of factors depending on the configuration of the network. As with any networking technology, it is important to understand the operational characteristics of VLANs if they are to be implemented within your network. This understanding will help to both implement well-designed VLANs and reduce the amount of time required to troubleshoot problems, should they occur.

Table of contents

FLUKE networks

Why use VLANs?

There are several reasons a network administrator may want to create one or more logical groupings of devices. In most cases, these reasons are broadcast control, security, Layer-3 address management, and consolidation of networking resources.

Broadcast control

As the number of devices within a broadcast domain increases, so does the broadcast rate within that broadcast domain. The broadcast rate is significant, since each device must process each broadcast to determine whether the contents of the broadcast should be pushed up the protocol stack.

For each broadcast that is received, the receiving device must interrupt the CPU to evaluate the contents of the broadcast frame. These interruptions take processing time away from other tasks running on the CPU and can increase the amount of time it takes for those tasks to complete.

An important aspect of VLANs is that broadcasts transmitted in one VLAN are not propagated to other VLANs. By limiting the number of devices in each VLAN, the broadcast rate within that VLAN can also be limited. An average number of broadcasts should be 30 broadcasts per second, or less. While no officially sanctioned quantity is specified in standards documents, field performance monitoring suggests that broadcasts should not exceed about 30 broadcasts per second.

Security

There are times when an organization needs to limit access to a specific device or devices on the local area network. If all of the devices within that organization are within the same broadcast domain, it becomes very difficult to limit this access. By placing devices in different broadcast domains, it is possible to limit access through the use of address filters and access lists.

For traffic to pass from one VLAN to another, the traffic must pass through a Layer-3 routing device. These routing devices allow you to specify which devices may access other devices. The use of this access control capability allows access to sensitive devices to be controlled and monitored.

Layer-3 address management

Creating IP subnets based on device type is a common design in local area networks. Printers may be assigned to one IP subnet, while workstations and servers belonging to the accounting group are assigned to another subnet. While logically this makes sense, deploying this architecture across a large local area network can prove to be impractical without the use of VLANs.

Consolidation of resources

Let’s take, for example, the use of a single subnet for all of the printers at a location. Each printer must be in the same broadcast domain as all of the other printers. This would require a separate switch on each floor for just the printers. These switches would have to be interconnected using a separate pair of copper or fiber, and this printer network would have to be connected to its own router interface.

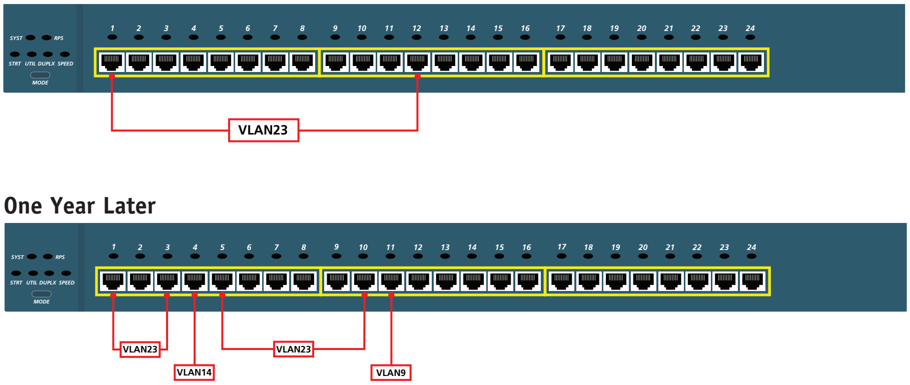
The use of VLANs allows the printers to be connected to the same switches as other devices on the network, share the same interconnecting copper or fiber and share the same router interfaces.

VLAN challenges

One of the greatest challenges when using VLANs within a local area network is documentation. When connecting a device to a switch, there is no easy way to know which VLAN has been assigned to the port, or whether the port has been configured to be a VLAN trunk. In most cases, the only way to determine the VLAN configuration of a switch port is to Telnet into the switch and display the configuration of the switch port in question. This process requires the appropriate login passwords and knowledge of the configuration commands for the specific switch and manufacturer.

As adds, moves and changes occur within a network, this challenge becomes even greater. When the switch was originally deployed, the policy may have been to assign the first 12 ports of each slot to VLAN23. However, as time passed, network administrators may have altered these assignments due to a lack of available ports, or a lack of understanding of the company standards. Either way, when connecting a new device to the switch, there is no longer a guarantee that the first 12 ports belong to VLAN23.

Original configuration



One Year Later

Figure 1

One of the benefits of VLANs is the ease in which ports can be moved from one VLAN to another. At the same time, this is one of the greatest problems with maintaining network documentation in a VLAN environment. It is so easy to reconfigure ports that the changes are rarely tracked and result in connectivity problems down the road. A simple and easy-to-use method of documenting the as-is VLAN configuration is needed.

VLAN best practices

Healthy VLANs don't just happen. They are carefully designed and maintained with the goal of optimum performance in mind. If attention is not paid to the design of VLANs, the resulting network will be overly complicated and difficult to maintain and troubleshoot.

Determine reasons for using VLANs

Four possible reasons for using VLANs were outlined at the beginning of this document: broadcast control, security, Layer-3 address management and consolidation of network resources. When designing a VLAN network, each of these reasons should be carefully explored. For example, if all of the users within your environment need access to all of the servers and network devices, security would not be a reason for implementing VLANs.

However, if you are implementing a Voice Over Internet Protocol (VoIP) solution, putting the voice traffic on one VLAN and the data frames on another might be a good reason for implementing VLANs. By separating these two types of traffic, quality of service can be applied to the voice traffic to reduce jitter and packet loss.

Use VLANs to reduce router hops

In order for frames to get from one VLAN to another, a Layer-3 device must route them. This device could be a traditional router, or a Layer-3 switch. Each router hop adds additional latency to the time it takes to get the frame from the sender to the receiver and can act as a bottleneck.

The goal in designing a VLAN network should be to put as many of the resources needed by a device on the same VLAN as the device. Using VLANs permits physically centralized hardware, while at the same time using VLANs to keep the server logically closer to the clients. This allows the client device to access the resource directly through the switched network without having to pass through a router. Being that a single VLAN can appear on multiple switches within a campus, a server in the data center can be on the same VLAN as a client several buildings away. A common design in many networks is to put all of the servers on the same VLAN. Unfortunately, this requires all of the clients to pass through at least one router to access the servers. While it makes IP address management easier, it introduces additional latency and potential bottlenecks.

Keep the number of VLANs to a minimum

There is a tendency to create more VLANs than necessary. While the switches themselves can support thousands of VLANs, the addition of each VLAN can create additional overhead for routers and other network devices.

An example of this was a network in a 42-story building. A VLAN was created for each floor, with additional VLANs for switch management and a server backbone. This network was running both IP and IPX protocols. In total, there were more than 2,000 IPX services throughout the local area network including printers, disk and time services.

Every 60 seconds, the router would send out Service Advertising Protocol (SAP) packets on each of the VLANs. Each of these packets contained 7 services. This resulted in 286 SAP packets being sent out on each broadcast domain every 60 seconds. With a total of 46 VLANs, the router had to send out more than 13,000 SAP packets every minute. It was found that if the router had to send out more than 2,000 frames, it would begin suffering CPU problems. While the switches could support the 46 VLANs, it was found that the router was not able to support that many.

Types of VLANs

There are three common methods used to assign a device to a VLAN:

1) Port based VLANs
2) Protocol based VLANs
3) MAC based VLANs

Port based VLANs

For port based VLANs, a switch port is manually configured to be a member of a specific VLAN. Any device connected to this port will belong to the same broadcast domain as all other ports configured with the same VLAN number.

The challenge of port based VLANs becomes documenting which port belongs to each VLAN. The VLAN membership information is not displayed on the front of the switch. As a result, the VLAN membership cannot be determined just by looking at the physical switch port. Only by looking at the configuration information can the membership be determined.

Protocol based VLANs

With Protocol based VLANs, the Layer-3 protocol being carried by the frame is used to determine VLAN membership. While this may work in multi-protocol environments, in a predominately IP based network, this method is not practical.

MAC based VLANs

One problem with port based VLANs is that if the original device is removed from the port and another device is connected, the new device will be in the same VLAN as the original. In the previous example of the printer VLAN, let's say a printer was removed from a switch port and an accounting device was connected to the empty port. The accounting device would now be in the printer VLAN. This may limit the access the accounting device has to resources on the network.

MAC based VLANs are intended to resolve this problem. In a MAC based VLAN, the VLAN membership is based on the MAC address of the device, not the physical switch port. If a device is moved from one switch port to another, the VLAN membership will follow the device.

Unfortunately, the correlation of MAC address to VLAN is a very time consuming process and this type of VLAN is rarely used.

VLAN tagging

VLAN tags are used to indicate VLAN membership within a frame going across the network. These tags are attached to the frame as it enters a switch port belonging to a VLAN and the tags are removed when the frame leaves a port belonging to the VLAN. The type of port within the VLAN will determine whether the VLAN tag is stripped from the frame or whether it remains attached to the frame. The two port types within a VLAN environment are known as access ports and trunk ports.

Access ports

Access ports are used where a frame enters or exits the VLAN. When an access port receives a frame, the frame does not contain a VLAN tag. As the frame enters the access port, the VLAN tag is attached to the frame.

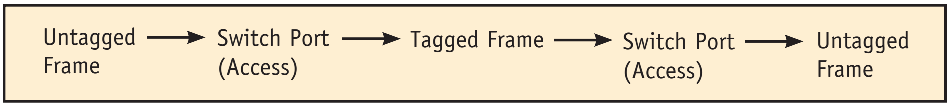


Figure 2

While the frame is within the switch, it carries the VLAN tag that was attached when it entered through the access port. As the frame leaves the switch through the destination access port, the VLAN tag is removed. The transmitting device and the receiving device are not aware that the VLAN tag was ever attached.

Trunk ports

In networks containing more than one switch, it becomes necessary to be able to send VLAN tagged frames from one switch to another. The difference between trunk ports and access ports is that trunk ports do not strip off the VLAN tag before sending the frame. With the VLAN tag preserved, the receiving switch will know the membership of the transmitted frame. This frame can then be sent out the appropriate ports on the receiving switch.

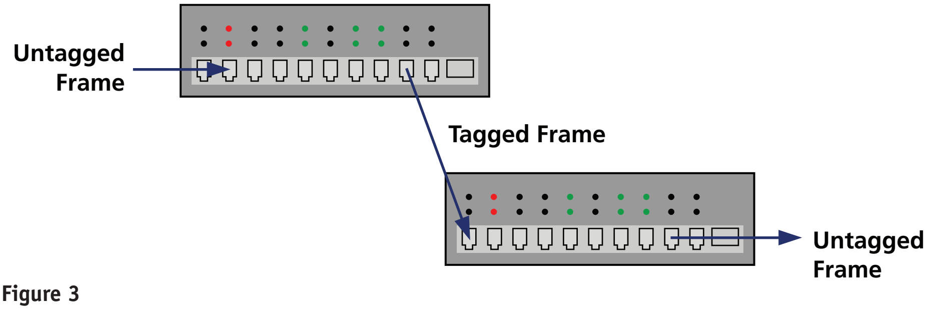


Figure 3

VLAN tagging technologies

Each VLAN tagged frame contains fields that denote its VLAN membership. There are two predominant formats for the VLAN tags, Cisco's Inter-Switch Link (ISL) format and the standardized 802.1Q format.

Cisco ISL

The Inter-Switch Link format is a Cisco proprietary VLAN tag format. When used, this VLAN tag adds 26 bytes of information to the front of each frame and appends a 4 byte CRC to the end of the frame. The format of this tag is as follows:

# of bits	40	4	4	48	16	24	24	15	1	16	16	8 to 196600 bits (1 to 24575 bytes)	32
Frame field	DA	TYPE	USER	SA	LEN	AAAA03	HSA	VLAN	BPDU	INDEX	RES	ENCAP FRAME	FCS

DA	Contains a multicast address of either 0x01-00-0C-00-00 or 0x03-00-0c-00-00
TYPE	Indicates the topology used to carry the encapsulated frame
USER	Four bit field indicates the user assignable priority of the frame
SA	The MAC address of the switch port that is transmitting this ISL tagged frame
LEN	The length of the encapsulated frame. This length field excludes the ISL header and ISL FCS fields
AAAA03	Constant field
HSA	High bits of source address – Must be 0x00-00-0C
VLAN	15 bit field used to indicate VLAN membership
BPDU	One bit field set to 1 if the encapsulated frame is a 802.1D Spanning Tree Bridge Protocol Data Unit
INDEX	Contains the port index of the transmitting switch port
RES	Reserved for Token Ring or FDDI encapsulated frames
ENCAP Frame	The entire unmodified frame as it was received by the access port
FCS	Frame Check Sequence for the ISL frame

Figure 3

802.1Q standards based tags

While ISL is a Cisco proprietary format, 802.1Q is an IEEE standardized format. The 802.1Q format is designed to allow VLAN tagged frames to pass between switches from multiple vendors. The 802.1Q tag contains fewer fields than the ISL tag and is inserted into the frame as opposed to being put at the beginning of the frame.

# of bits	48	48	16	3	1	12	16	368 to 12000	32
Frame field	DA	SA	8100	Priority	CFI	VLAN	Ethertype	Data	FCS

DA	Destination address of the frame. This address is the same in the tagged frame as it is in the untagged frame.
SA	Source address of the frame. This address is the same in the tagged frame as it is in the untagged frame.
8100	Constant field indicates that this frame contains an 802.1Q VLAN tag
Priority	Three bit user defined priority field
CFI	Canonical Format Indicator – One bit field indicates whether options follow the VLAN tag. Primarily used in Token Ring networks.
VLAN	This 12 bit field is used to indicate the VLAN membership of the tagged frame
Ethertype	Indicates the Layer-3 protocol contained in the tagged frame
Data	The data portion of the tagged frame
FCS	The data portion of the tagged frame

Figure 4

Maintaining VLANs

One of the greatest challenges in a network that employs VLANs is the maintenance of the VLAN configuration across multiple switches. Without a centralized means of configuring and maintaining the VLAN information, the network administrator must configure the VLANs on each switch individually. Cisco has developed a protocol known as the VLAN Trunk Protocol to help overcome some of these shortcomings.

VTP – VLAN Trunk Protocol

The VLAN Trunk Protocol (VTP) allows you to configure VLANs on a single device, the VTP server, and have this configuration information propagated out through the switched network. This reduces the amount of time required to administer the VLANs.

Within a VTP environment, a switch can be in one of three different roles. The switch can operate as a VTP server, a VTP client, or it can be in transparent mode. This role will determine how the VLANs are configured on the switch.

The VLAN Trunk Protocol has the capability to support multiple VTP domains. The client switches in each VTP domain receive their configuration information from that domain's VTP server. It is possible to have multiple VTP domains within the same local area network.

VTP server

The VTP server is the root of each VTP domain. The server is the only switch in the domain that can add, delete and rename VLANs within the VTP domain. When an un-configured Cisco switch is first turned on, it will start in VTP server mode. The default configuration must be changed to put the switch into one of the other two modes.

The VTP server will periodically advertise the VTP domain name, the VLAN configuration and provide the most current configuration revision number. This revision number is used to ensure that all of the switches that are part of the VTP domain have the most current and accurate VLAN configuration information.

When VLANs are created on the VTP server, they are stored in the server's NVRAM with all of the other VLAN configuration information. When the switch is reset, this configuration information is retained.

VTP client

The VTP client switches will receive all of their VLAN configuration information from the VTP server switch. The client switches cannot add, delete or rename VLANs. To add a new VLAN to a client switch, the VLAN must be added to the VTP server. This new VLAN will then be propagated out to all of the client switches. After the new VLAN has been added, ports on the client switch can then be associated with the new VLAN.

Like the VTP server, the client switch stores the VLAN configuration in NVRAM. However, unlike the VTP server, when the client switch is reset, all of this configuration information is lost. After the switch is reset, it will send a VTP information request to the VTP server to acquire the current VLAN configuration.

VTP transparent

VTP transparent switches differ from VTP client switches in that VLANs can be configured manually on these switches. If configured to be part of a VTP domain, they can receive VLAN configuration information from the VTP server. They will not, however, inform the VTP domain of the locally configured VLANs.

Switches configured to operate in VTP transparent mode will receive VTP configuration frames and pass these frames out all trunked ports. This allows VTP client switches to be connected to the VTP transparent switch. The client switches will still be able to exchange VLAN configuration information with the VTP server through the transparent switch.

VTP data frames

The data frames used to configure and maintain a VTP domain can be encapsulated in either 802.1q or ISL frame formats. VTP uses a reserved multicast address as the destination for all data frames. This multicast address is 0x01-00-00-0C-CC-CC-CC with a Logical Link Control code of Sub Network Access Protocol (SNAP) and a type code of 2003 in the SNAP header. Each data frame contains a VTP header and a VTP message type. (Note in the following descriptions, the frame formats show the VTP message only and not the complete Ethernet frame.)

There are three types of VTP messages:

1) Summary
2) Subset
3) Request

Summary frames

Summary frames are sent by both VTP servers and VTP clients every five minutes and immediately after each change to the VTP domain. This summary advertisement contains basic information about the VTP domain and the configuration revision. The summary frame may be followed by a number of detail frames known as Subsets.

The summary frame format is shown below.

# of bits	8	8	8	8	256	32	32	96	128
Frame field	Version	Code	Followers	Management Domain Length	Management Domain Name	Configuration Revision Number	Updater Identity	Update Timestamp	MD5 Digest

Version	VTP version number
Code	Indicates message type
Followers	Indicates the number of subset frames that follow this summary frame
Management Domain Length	Length of management domain name
Management Domain Name	Name of VTP domain
Configuration Revision Number	Current revision number for the VTP configuration. This number starts a 0 and increments each time there is a change to the VTP configuration
Updater Identity	IP address of the device that caused the most recent update to the configuration revision number
Update Timestamp	Timestamp indicating the time at which the most recent update to the Timestamp configuration revision number was received
MD5 Digest	MD5 digest value over the secret value and all VLAN information

Figure 5

Subset frame

Subset frames are used to provide detailed information about each of the VLANs within a VTP domain. These frames may be sent out as part of a configuration change or in response to a VTP request frame.

# of bits	8	8	8	8	256	32			
Frame field	Version	Code	Sequence Number	Management Domain Length	Management Domain Name	Configuration Revision Number	VLAN Info1	VLAN Info...	VLAN InfoN

Version	VTP version number
Code	Indicates message type
Followers	Indicates the number of subset frames that follow this summary frame
Management Domain Length	Length of management domain name
Management Domain Name	Name of VTP domain
Configuration Revision Number	Current revision number for the VTP configuration. This number starts at 0 and increments each time there is a change to the VTP configuration.
VLAN Info	Each VLAN information field contains detailed information for the VLANID.

Figure 6

Request frame

VTP clients send request frames to VTP servers. These frames are sent when one of the following conditions occur:

- The VTP domain name is changed
- The VTP client receives a summary advertisement with a higher configuration revision number than its own
- A subset frame is missed
- The switch is reset

The VTP server will respond to the request frame with a summary frame and as many subset frames as it takes to satisfy the request.

# of bits	8	8	8	8	16
Frame field	Version	Code	Reserved	Management Domain Length	Start Value

Version	VTP version number
Code	Indicates the type of VTP advertisement
Followers	Reserved field
Management Domain Length	Length of VTP domain name
Start Value	VLANID of the first VLAN for which information is requested. The VTP server will respond with subset frames containing information about all VLANs equal to and greater than the start value. If a start value of 0 is specified, information about all VLANs will be provided.

Figure 7

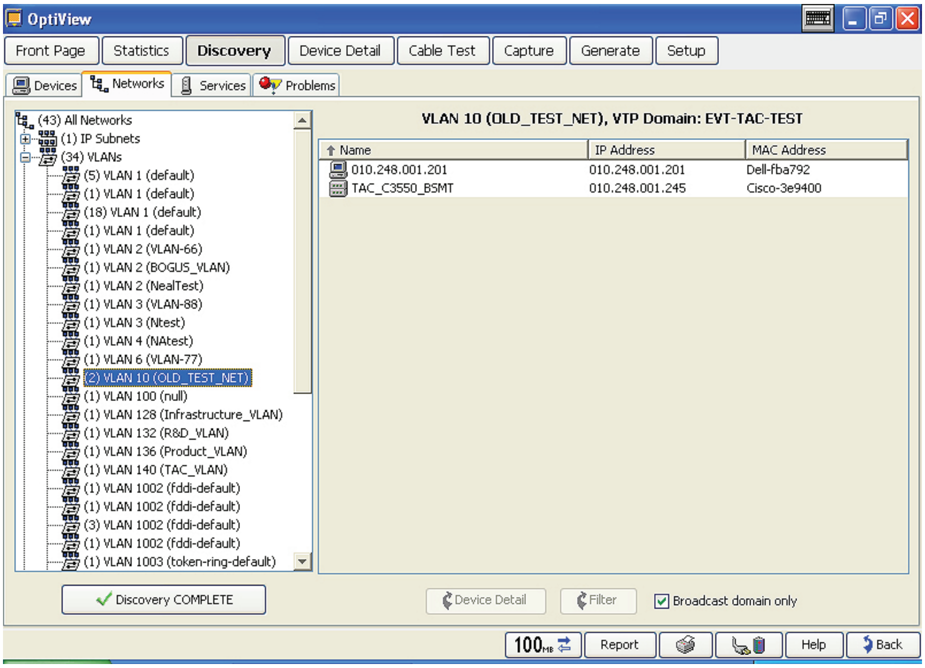
Conclusion

As the use of virtual LAN technology has become common, designing and maintaining networks must now account for the presence of VLANs. That's where best practices and tools come in to help set up your VLAN and keep it healthy. Any network engineer or manager first needs to understand how and why VLANs work within the network and institute good documentation practices in order to effectively troubleshoot problems and optimize VLAN performance. Taking advantage of tools designed to gather and display VLAN-specific information can drastically reduce equipment costs and troubleshooting times.

How the OptiView Series III analyzers make deploying and managing VLANs easier

All the functionality of multiple tools is combined into one device, allowing the network engineer to overcome the challenge of documenting the VLAN configurations on the network and the specific configuration of a switch. In addition to verifying correct VLAN port assignments on each switch, there are a number of other potential issues that must be considered such as:

- Are all the devices in the correct VLANs or are there servers or other devices in VLANs where they do not belong?
- Is the traffic on each VLAN at expected levels?
- Is the traffic on trunk or uplinks at expected levels?



```
(43) All Networks
  (1) IP Subnets
  (34) VLANs
    (5) VLAN 1 (default)
    (1) VLAN 1 (default)
    (18) VLAN 1 (default)
    (1) VLAN 1 (default)
    (1) VLAN 2 (VLAN-66)
    (1) VLAN 2 (BOGUS_VLAN)
    (1) VLAN 2 (NealTest)
    (1) VLAN 3 (VLAN-88)
    (1) VLAN 3 (Ntest)
    (1) VLAN 4 (NAtest)
    (1) VLAN 6 (VLAN-77)
    (2) VLAN 10 (OLD_TEST_NET)
    (1) VLAN 100 (null)
    (1) VLAN 128 (Infrastructure_VLAN)
    (1) VLAN 132 (R&D_VLAN)
    (1) VLAN 136 (Product_VLAN)
    (1) VLAN 140 (TAC_VLAN)
    (1) VLAN 1002 (fddi-default)
    (1) VLAN 1002 (fddi-default)
    (3) VLAN 1002 (fddi-default)
    (1) VLAN 1002 (fddi-default)
    (1) VLAN 1003 (token-ring-default)
```

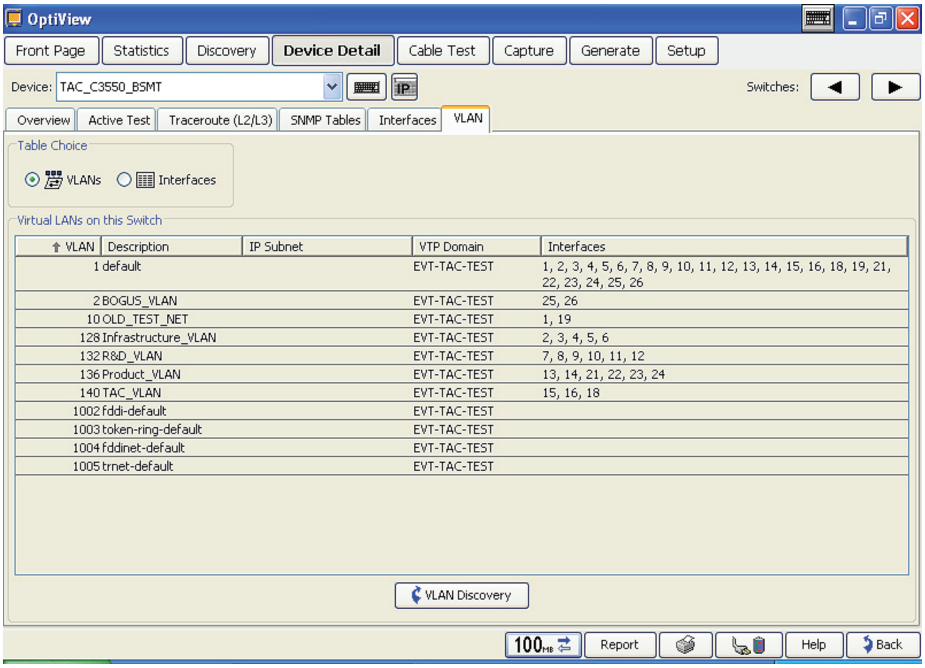
VLAN 10 (OLD_TEST_NET), VTP Domain: EVT-TAC-TEST

Name	IP Address	MAC Address
010.248.001.201	010.248.001.201	Dell-fba792
TAC_C3550_BSMT	010.248.001.245	Cisco-3e9400

☑ Broadcast domain only

Figure 8

The advanced active network discovery techniques used by the OptiView Series III analyzers, automatically identifies the VLANs on the network together with the devices participating in those VLANs. The vendor independent infrastructure analysis makes verification of switch port configurations easy – In addition to identifying the VLAN number, the OptiView Analyzers also provide details on the VLAN Name, IP subnet, VTP domain and a list of interfaces associated with each VLAN. The analyzer will also determine which ports are configured as trunk ports and uplink ports.



Device: TAC_C3550_BSMT

Table Choice

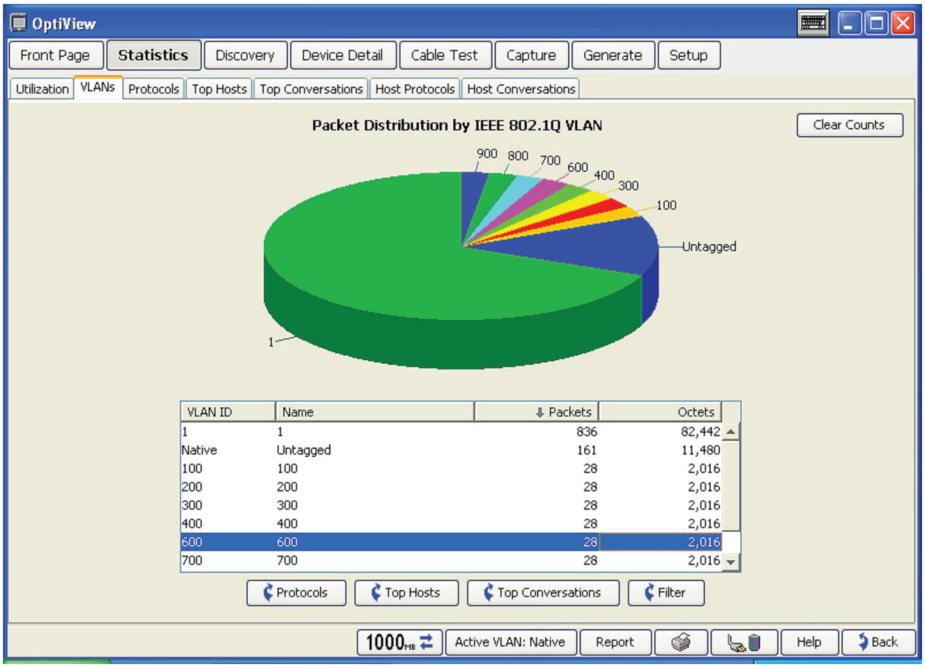
● VLANs ○ Interfaces

Virtual LANs on this Switch

VLAN	Description	IP Subnet	VTP Domain	Interfaces
1	default		EVT-TAC-TEST	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 21, 22, 23, 24, 25, 26
2	BOGUS_VLAN		EVT-TAC-TEST	25, 26
10	OLD_TEST_NET		EVT-TAC-TEST	1, 19
128	Infrastructure_VLAN		EVT-TAC-TEST	2, 3, 4, 5, 6
132	R&D_VLAN		EVT-TAC-TEST	7, 8, 9, 10, 11, 12
136	Product_VLAN		EVT-TAC-TEST	13, 14, 21, 22, 23, 24
140	TAC_VLAN		EVT-TAC-TEST	15, 16, 18
1002	fddi-default		EVT-TAC-TEST	
1003	token-ring-default		EVT-TAC-TEST	
1004	fddinet-default		EVT-TAC-TEST	
1005	trnet-default		EVT-TAC-TEST	

Figure 9

The ability to display VLAN configuration information is available not only for switches that are in the same broadcast domain as the analyzer, but for any switch that is accessible via IP from the OptiView Network Analyzer. This means that the VLAN capabilities can be used to display the VLAN configuration of a switch located many router hops from the analyzer.



Active VLAN: Native

VLAN ID	Name	Packets	Octets
1	1	836	82,442
Native	Untagged	161	11,480
100	100	28	2,016
200	200	28	2,016
300	300	28	2,016
400	400	28	2,016
600	600	28	2,016
700	700	28	2,016

Figure 10

With inter switch trunks being widely deployed and now access trunks to the desktop are becoming more common, especially in VoIP deployments that support multiple broadcast domains together with both tagged and untagged traffic, it is essential to be able to see each VLAN on the trunk port together with the traffic levels of each VLAN on the trunk. It is also necessary to be able to identify the protocols in use on each VLAN together with the top hosts and conversation pairs on the VLAN in order to arm network managers with actionable VLAN information to instantly identify and overcome challenges and issues that could ordinarily take valuable time and resources to solve.

The business case for integrated network analyzers

The OptiView Series III Network Analyzers help network professionals manage IT projects, solve network problems and support IT initiatives, resulting in reduced IT costs and improved user satisfaction. They give you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network. No other tool offers this much vision and all-in-one capability to help you:

- Deploy new technologies and applications
- Manage and validate infrastructure changes
- Solve network and application performance issues
- Secure the network from internal threats

They show you where your network stands today and helps you accurately assess its readiness for the changes you need to make now and in the future. Leverage the power of the OptiView Analyzers to give you vision and control of your network. To learn more about OptiView, go to **www.flukenetworks.com/optiview**.

Printed in U.S.A. 5/2008 2140095 H-ENG-N Rev B