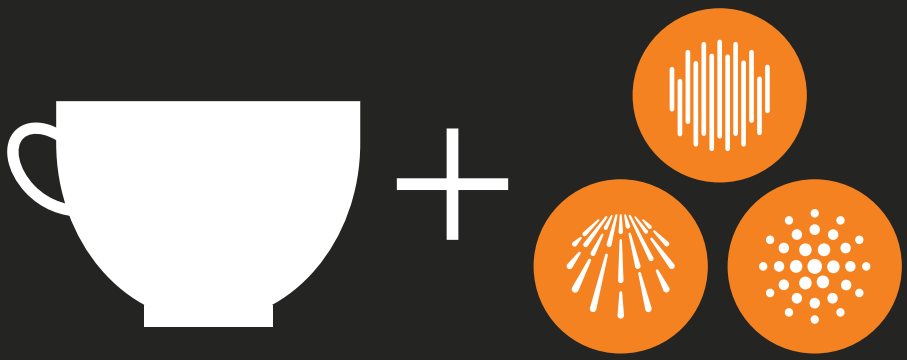
VLAN security over a coffee



Business Services

orange™

editorial

For years now, plugging in to a wired network has been the norm when accessing corporate computer resources.

When ethernet was first introduced, a physical separation existed. This guaranteed a high level of security through the isolation of the different networks. But as our computer needs evolved, a new kind of technology was needed to maintain a consistent level of isolation between each workflow: Virtual Local Area Networks (VLAN).

We now use VLANs to logically segment networks located on a single physical medium.

However, this implies a certain amount of risk. In addition to the risks posed by separate physical networks (etherpin use, for example), other risks have emerged. The present collection of blog posts aims to help you understand and combat VLAN security risks, so you can best protect against and combat the most common “basic” attacks.

Guillaume Bazire

content

ethernet is important, too!

by Pascal Bonnard

Today, the media provides rather extensive coverage on the latest malicious web attacks, so most level 3 risks and above have been identified and widely documented. But this doesn't hold true for risks associated with lower levels, especially risks on local networks.

A LAN is a local area network typically associated with RJ45 ethernet outlets. For this reason, people often speak about LAN security and facility security in the same breath. However…

security inside the office…

Inside the office, local networks are highly vulnerable:

- to start with the obvious: **how many wall outlets** are there in your office and where are they located?
- what do the cables plugged into them connect to?
- a bit more difficult: how do you monitor the equipment connected to the LAN?
- how can you spot unmonitored **replication equipment** when switches are mass-market products available for just a few dollars?
- can you check if any PLC device is plugged in?

…and outside

Outside the office walls, companies often extend LANs using wireless equipment, such as WiFi.

As for “official” WiFi access points, you can find plenty of articles elsewhere pertaining to specific questions about security. But let’s not forget that WiFi boosting equipment is also available on the mass market. And this equipment is easy to set up and hard to spot. That means a **LAN’s range can be uncontrollably boosted.**

That’s how you can use the same network to play computer games with your friend in a building across the street from yours.

Also outside the office, **high-performance level 2 transport services** have become more effective over long distances. Not only does WAN transport IP flow, but it now transports level 2 flow as well.

conclusion

For these reasons, it’s crucial to **address level 2 security questions**. And that’s what we’ll do in the following blog posts!

the blog post online
http://oran.ge/T5sUM6

VLAN hopping: a successful technique

par Pascal Bonnard

Attention: if you think **VLAN = security, this article just might burst your bubble! VLAN security is less extensive than LAN security,** and it decreases with:

- cable length
- the presence of “Jim” and “Pam”
- the number of ports

using a simple ethernet cable to connect two VLAN

Experts will tell you that a switch alone can’t connect two VLAN. To do so, they’ll say, you need a router switch, and it needs to be a Level 3 VLAN. Big mistake!

In truth, **a lone switch can connect two VLAN**, you just need a little cable. And you can do it all on level 1. In fact, as Groucho Marx would say, “Why, this is so simple, a five-year-old child could understand it! (Go find me a five-year-old child; I can’t make heads or tails of it.)”

Imagine a switch with two user VLANs. Let’s say VLAN 2 and 3. The first 12 ports are in VLAN 2, the next 12 in VLAN 3. The PC of one employee—we’ll call him Jim—is on port 1, and his colleague, Pam’s PC is on port 20. Jim plugs in an **ethernet cable** between port 12 and port 24. Now VLAN 2 and 3 are connected. As long as the IP addresses aren’t duplicated, now

Jim can start up an office romance with Pam!

For 2013, I'll let you in on a "VLAN hopping " hack that really works.

trick of the trade: an ethernet loop for dummies

Sometimes you need to use "loops" to make a network run properly. For example, you might need to do so when you're trying to solve certain IP address problems. My colleagues call this a "hairpin."

So last Christmas I asked for a marvelous "Etherpin" to connect two VLANs. Here's what it looks like:

Etherpin

ethernet loop: the CPL version

To use his Etherpin, our pal Jim needs to access the switch, which is sometimes well hidden under his colleague Dwight's collection of bobble-head dolls. Since it's a hassle to push them out of the way, Jim just uses his PLC Etherpin. What will they think of next?

good to know

No one can continuously and reliably monitor a LAN's perimeter.

All he needs to do now is look around the office and find an available RJ45 Ethernet outlet that's also close to an electrical outlet.

All right , no more kidding around now; this part is serious.

I've already told you in my first post that no one can continuously and reliably monitor a LAN's perimeter. Maybe you thought of it as a trivial point at the time, but now you know it's an issue that deserves some thought.

so what can you do?

Jumping out the window is not an acceptable solution. Read the post again. At the beginning I mention LAN security. Actually, if Jim plugs his PC into a wall outlet in Pam's office, the end result will be about the same. As long as LAN resources are sufficiently protected, then using an Etherpin **will not radically alter the situation.**

In my opinion, trying to protect against an Etherpin isn't worth the trouble. Protecting your LAN is a lot more effective. One easy way to do this is to set up access controls for level 3 protocols and used IP addresses (Access Control List).

Make your resolutions for 2013. Monitor your level 3 protection, the ACLs you use in each switch, and your network routers. Overhaul the firewall. Review your intrusion detection system...

the blog post online
http://oran.ge/TI3C2R

what's a private VLAN?

by Guillaume Bazire

For several years now, I've often turned to VLAN **to segment company networks on Level 2**. Each time, an IP subnet is attributed to these VLANs and routed through Level 3 equipment (such as routers or a firewall).

But I have noticed that people often **take this segmentation too far**, slicing the network up into a plethora of subnets in the hope of ensuring enough security between all of the machines.

Private VLANs are there to **mitigate excess segmentation** by providing an extra layer of Level 2 security.

needs met by a private VLAN

The first need that comes to mind is using a PVLAN for **guest users** (in offices where employees use their PCs to connect, for example). This method is often used to provide guest WiFi access. An option that restricts communication between customers can be applied on the terminal, eliminating direct communication between them (by default, communication is broadcast on a WiFi network the same way it is on a Hub, so you need to protect against data theft).

In this example, the goal is to **avoid data transfer or attacks** between customers, even on "hostile" cable networks. Normally, if you want to isolate these customers, you have to use one VLAN per customer, which is unthinkable. Luckily we have private VLAN.

"private VLANs often simplify network architecture or provide extra security"

good to know

People often take Level 2 segmentation too far.

You could also use DMZ subnets, to a**void creating too many zones** on the firewall. We often need to segment DMZ servers by using an IP network and consequently an interface on the firewall (and the more interfaces on a firewall, the more volatile the traffic matrix).

solutions offered by a private VLAN

For my first need (a "guest" customer zone) security concerns dictate that it's best to isolate each individual customer from another. But this is precisely where, very often, security goes down the tubes, and everyone ends up on the same VLAN with unrestricted access.

Instead, use a private VLAN with **a guest PVLAN in "Isolated" mode**. That way you have just one VLAN for all guests, and by default they can only contact the gateway, which handles all filtering and/or authentication when accessing resources.

On to our second DMZ need. You often see DMZ servers used in proxy mode with LAN->DMZ->WAN or WAN->DMZ->LAN communication, but rarely any intra-DMZ communication. For a DMZ containing several types of services (relays for e-mail, internet, SSL portals, etc), any alteration of a DMZ server by a pirate will threaten all other services in the DMZ. That's why you often see strict separation applied between several DMZs.

With the private VLAN in "Isolated" mode, a single DMZ can contain several servers with different services but the same level of security for each one.

In the case of a group of servers that need to communicate with each other, **"Community" mode** would best fit. This option

makes it possible for servers to communicate within a single community and access the gateway (firewall), all while remaining isolated from servers in another community.

To sum up, instead of having x number of DMZs, each with its own IP network, you can have x number of PVLAN communities, each with a single IP network and a single interface on the firewall, for an equivalent level of security.

conclusion

Private VLANs, though known to many experts, are too often set aside even though they can **simplify network architecture** (for example, when isolating servers in a DMZ) or provide **extra security** that's easy to set up (for example, for guest networks).

Now that you know more about private VLANs, you just have to wait for the right opportunity and remember to use them! ;-)

the blog post online
http://oran.ge/UKsND5

private VLANs: an in-depth look

by Guillaume Bazire

It looks like my intro to private VLAN went over well, so I thought you might want to know more. I want to show anyone who's still hesitant that things aren't all that complicated once you get under the hood.

how it works

A private VLAN always includes **a primary VLAN** ("Promiscuous," as it contains "promiscuous ports") and one or **more secondary VLANs** (two kinds: "Isolated" and "Community," containing the "Host Ports").

Each different VLAN will be on the same IP subnet (since only the primary VLAN will have a Level 3 interface or connect to the gateway by default).

to sum up...

Three different types of VLAN make up a private VLAN infrastructure

- Primary (Promiscuous): one machine configured as the primary VLAN can communicate **with all other VLAN** on the private VLAN. This is typically used for routers and other shared services
- Isolated: **completely separate** at Layer 2 from other

machines on the same VLAN (including broadcasts). The only exception is communication with primary VLAN machines

- Community: machines in the same community can **communicate with each other** and with primary VLAN machines. However, machines in one community cannot communicate with machines in another community or with isolated VLAN machines

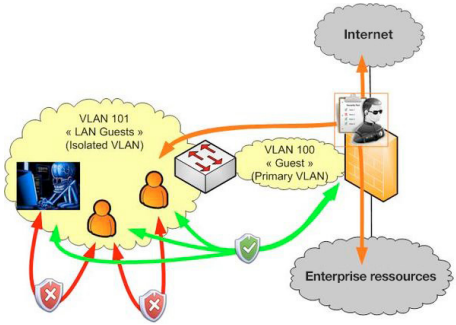
In practice, secondary VLANs are linked to a primary VLAN, which has at least an exit router or firewall.

concrete scenarios with examples

1. “guest” zone scenario

For guest zones, we saw in the last article that isolating customers is essential (especially since more and more corporate employees are BYOD-friendly). To ensure this isolation, put the customers in an isolated VLAN and put the firewall in a primary VLAN.

This chart should help make it clear:



This will ensure proper isolation for each customer and enable monitored communication with the rest of the network by the firewall.

good to know

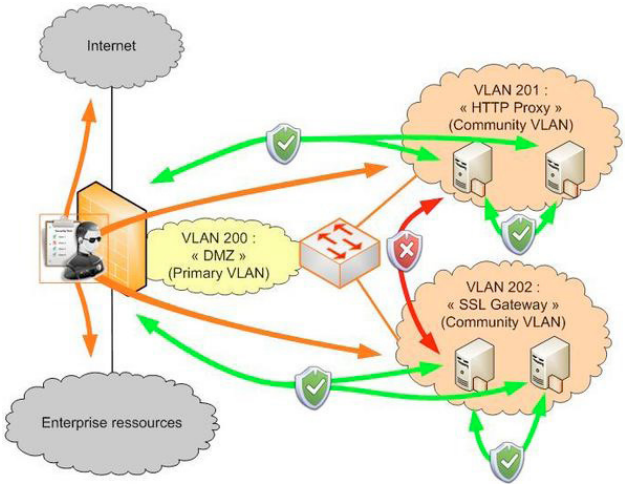
For guest zones isolating customers is essential.

2. “DMZ” zone scenario

As for DMZ zones, the goal is to avoid having too many zones that each add extra interfaces (or sub interfaces) on the firewall.

One way to do so is to have proxy servers and SSL gateways in separate community VLANs, while still keeping your firewall in a primary VLAN.

Here’s what it looks like:



Here our servers can communicate directly within their community, but not with other communities. They share one common resource, namely the firewall, which monitors access to the rest of the network: LAN, WAN, and even other DMZ communities (if you authorize the firewall to enable and monitor communication between interfaces)

did that help clear things up about private VLANs?

I hope these two short articles have explained some of what private VLAN technology involves. Now you should be able to use this technology in your designs and add a little **extra layer of security** to your infrastructure.

the blog post online
http://oran.ge/SwYdMK

about the author

Guillaume Bazire

I work at Econocom, where I'm currently a security architect for Cloud France solutions and its transversal services for Orange Business Services. I'm still new to the blog. My background is in networks and I've specialized in security since 2008. A huge technology buff with experience as a security integrator, I'm excited to contribute to the blog.

Pascal Bonnard

I've worked on engineering Ethernet switches since 2004. I'm curious by nature, so I wanted to check out what was under the hood, and that's where I found a mess of protocols. Although they might be there for good reasons, they still pose a lot of security issues. Are they reliable? Can they be mistaken? To me, it seems like this field is rarely covered, while the little information that is available is insufficient and often incorrect. So I want to share what I know, mainly based on lab tests and several hundred operational machines.

Our blog :
http://blogs.orange-business.com/connecting-technology/

Document available for download at :
http://knowledge-center.orange-business.com/

Edited by Orange Business Services
27.11.2012

Business Services

orange™

France Télécom – 78, rue Olivier de Serres, 75015 Paris, France – SA au capital de 10 595 541 532 – 380 129 866 RCS Paris – Document non contractuel – juin 2012