

FI:PV204 Laboratory of Security and Applied Cryptography II

Network Segmentation

Valdemar Švábenský

March 18, 2014

Network segmentation is a process of splitting a computer network into subnetworks called network segments. A segment is a physical network construction. Its boundaries are established by devices capable of regulating the flow of packets into and out of the segment, including routers, switches, hubs, bridges, or multi-homed gateways (but not simple repeaters).

Advantages of segmentation

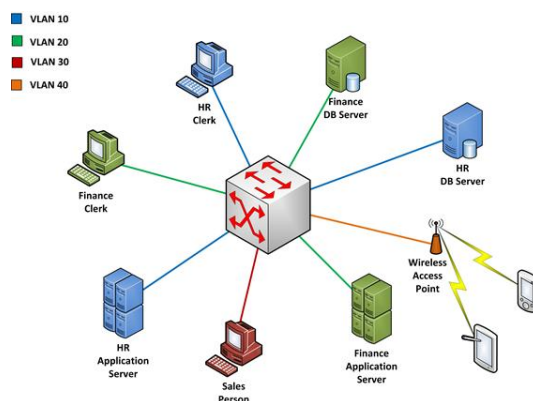
The main advantages are improved performance and improved security.

- Local traffic on a segmented network is minimized, because there are fewer hosts per segment.
- Internal network structure is not visible from outside.
- Related computers are physically separated into groups based on their security classifications.
- User access to sensitive data is limited and controlled.
- Local failures inside a segment do not affect other parts of network.
- Broadcasts will be contained to local network.
- It is easier to manage a large network of users and simplifies the application of firewall rules.

In order to realize these benefits, the network must maintain strict separation of each segment and be very precise on the traffic that is allowed between segments. A policy enforcement device (router running ACLs, firewall, or IPS solution) between segments defines what users can and cannot access on other segments.

Example

In traditional networks, perimeter defenses protect the data center from external threats with little protection against internal threats. Once on-the-wire, an attacker has free access to system attack surfaces. The most common way to segment traffic from a wireless network without obscuring the traffic on the wire is using virtual local area networks (VLANs). It creates a collection of isolated networks within the data center. Authorized users only see the servers and other devices necessary to perform their tasks.



The figure shows how a single switch manages four collections of devices. A VLAN is a set of switch ports. The HR clerk and the HR servers are assigned to switch ports 2, 4, and 8. Ports 2, 4, and 8 are configured as VLAN 10. Devices connected to these ports can talk to each other, but they are logically isolated from devices connected to ports not part of the VLAN 10 set.

The sales person's desktop on VLAN 30 is unable to communicate with any other devices on the network. If the computer sends an ARP broadcast requesting the MAC address of the HR application server, for example, the request never reaches VLAN 10. Because the desktop cannot obtain the server's hardware address, no connection is possible.

Implementation

Traditionally, wireless network segmentation has been accomplished by creating multiple Service Set Identifiers (SSIDs) and mapping each to a different VLAN. Although this option has support in almost every Wi-Fi product, it is not suitable for complex networks. Creating separate SSIDs for each security scenario degrades network's performance and suffers from lack of scalability.

A single SSID can be used for all similarly capable device classes, such as all devices that support WPA2 authentication. User roles do not necessarily need different SSIDs (although a few SSIDs may still be required to support varying authentication and encryption methods).

The other common way to segment is through tunnels. However, this approach has some major performance drawbacks, since a tunneled network is only as fast as the tunnel terminator (controller in a wireless network). Moreover, many AP tunnels have an encrypted payload, making it impossible to check packets for viruses and attacks.

A third method of segmenting is a MAC firewall, which is like a MAC filter but instead of enforcing a client MAC or source MAC it can also filter on destination MAC. A properly configured firewall will segment users, control access and traffic, and provide detailed reporting.

Configuring VLANs

When a VLAN set is configured as private (isolated), none of the ports in the VLAN set can communicate with each other. Servers can communicate with users from other VLANs, but security is strengthened by preventing the servers from establishing session with each other. The most common attacks against VLAN technology, VLAN hopping and double 802.1Q tagging, are preventable with proper attention to configuration best practices.

Q-switches can use two types of access control lists: basic ACLs and VACLs. ACLs filter packets entering a L2 interface. If a defined ACL entry denies a certain source/destination/protocol set, any packet containing it is dropped. VACLs are assigned to VLANs. Once assigned, a VACL filters all traffic entering the VLAN. The switch checks ACLs from the top down, applying the first match it finds based on the packet content. If no match is found, a default deny is usually applied and the packet is dropped.

Sources

- <http://www.revolutionwifi.net/2011/01/wireless-network-segmentation-options.html>
- <http://resources.infosecinstitute.com/vlan-network-chapter-5/>
- http://aerohive.com/pdfs/Aerohive-Whitepaper-Building_Secure_Wireless_LANs.pdf
- http://compnetworking.about.com/od/networkdesign/1/bldef_segment.htm