Lecture 10:

Virtual LANs (VLAN)
and
Virtual Private Networks (VPN)

Prof. Shervin Shirmohammadi
SITE, University of Ottawa

Virtual LANs

• Description:
  – Group of devices on one or more physical LANs that are configured as if they are logically attached to the same wire
  – LAN’s based on Logical instead of Physical connections
• Used to help alleviate traffic congestion without adding more bandwidth
• Used to separate out users into logical groups of workers, regardless of actual physical location.
• Usage scenarios:
  – Say you want workers assigned to the same project to be grouped logically together for control of traffic but they are physically located in different physical areas
  – Say you want to divide up the broadcast domain in a large flat network without using a bunch of routers
• Must be supported by the switch: switches must have the ability to support more than one subnet
VLAN Types and Strategies

• Types:
  – Port Based - Configured at each switch port
    • Port X on Switch A belongs to VLAN 1
    • Port Y on Switch B belongs to VLAN 1
  – MAC Address Based - Uses the end stations MAC address for VLAN Assignment
    • Host X MAC belongs to VLAN 1
    • Host Y MAC belongs to VLAN 1
  – Protocol Based - Uses LAN protocol to determine VLAN assignment
    • Host X uses IP and belongs to VLAN 1
    • Host Y uses IPX and belongs to VLAN 2
  – Dynamic Based - A User Profile (stored as a database) determine VLAN assignment
    • When Host X logs in, the profile says to connect the user to VLAN 1

• Strategies:
  – At the User Level
  – At the Wiring Closet Level
  – AT the Distribution Switch Level

User Level VLAN

• Users belong to a specific VLAN regardless of where they attach to the network
• User can “roam” on the network
• Beneficial when traffic stays on the VLAN
• However, broadcast traffic will follow the user

Broadcast Domain for VLAN 1
User Movement

If Host A moves to a different Workgroup Switch, the Broadcast Domain follows the movement of Host A.

Wiring Closet VLAN

- Provides a means for broadcast domain control
- Good when traffic mostly flows to enterprise servers
- People must be physically close together on same VLAN
- Broadcast traffic will not follow the user
User Movement

If Host A moves to a different Workgroup Switch, it belongs to a new VLAN. Broadcast Domain stays with the switch, and does not follow Host A.

Distribution Switch VLAN

- Middle ground between User and Wiring Closet designs
- For traffic that goes to both enterprise and distributed services
- If users move but stay on the same distribution switch - Same VLAN
- If users move to different distribution switch, then it’s a Different VLAN
User Movement

If Host A moves to a different Distribution Switch, the Broadcast Domain follows Host A since it stays on the same distribution switch.

How Does the Network Know?

- How does the network know where to send the data when a VLAN has been put into place?
  - Initially, IEEE 802.10, “Interoperable LAN/MAN Security (SILS)” standard released in 1992, puts the VLAN information between the MAC and LAN address space. Today, using IEEE 802.1Q, Frames can be tagged with the VLAN information.

- How do we interconnect these smart switches?
  - We could try to manually connect them together.
  - This is not recommended. One can easily make a mistake when physically interconnecting the appropriate ports for the VLAN.
VLAN Trunking

- One simple solution is to **trunk** the lines together:
  - On each switch we configure a trunk port (can be any Ethernet port) that is logically connected to multiple VLANs.
  - Then we connect the trunk ports together.
  - The numbering is kept consistent through the use of 802.1Q tags.

- When one switch sends an Ethernet frame to the other, the transmitting switch inserts the 802.1Q tag with the appropriate **VID**.
- The receiving switch reads the VID and forwards the Ethernet frame to the appropriate VLAN.

![VLAN Trunking Diagram](image)

802.1Q Tag

- The priority bits are the reason why 802.1Q is often referred to as 802.1 P/Q
- The VID bits make trunking possible.
- Ethernet switches and endpoints must be capable of interpreting the 802.1Q tag to make use of the tag.
802.1Q Terminology

- **access port / link** - defines a port with one or more untagged VLANs, and a link connecting two such ports.
- **trunk port / link** - defines a port with multiple VLANs that are all tagged, and a link connecting two such ports.
- **hybrid port / link** - defines a port with both untagged and tagged VLANs, and a link connecting two such ports.
- **VID** - VLAN ID
- **PVID** - Port VLAN ID
- **tagged frame** - An Ethernet (IEEE 802.3) frame with the 802.1Q tag.
- **clear frame** - An Ethernet frame with no tag.
- **VLAN trunking** - a generic networking term to describe the process of forwarding multiple VLANs across a single link, whether via 802.1Q or proprietary protocols like Cisco’s InterSwitch Link Protocol (ISL).

VLAN Configuration

- The VLANs must be configured independently on each switch, using any of the following methods:
  - **manually** via the command line interface (CLI) or web interface.
  - with a VLAN management tool provided by the vendor.
  - **automatically** with a **standard** protocol like GVRP (GARP VLAN Registration Protocol), which works in conjunction with 802.1Q.
  - **automatically** with a **proprietary** protocol like Cisco’s VTP (Virtual Trunking Protocol), which works in conjunction with Cisco’s proprietary ISL (Inter-Switch Link) trunking protocol.
A VLAN Scenario

- The access switches have multiple VLANs, and the uplinks to the distribution switch are hybrid or trunk links.
  - VLAN1 is the management VLAN in this setup.
  - The access switches are hosts on VLAN1.
  - Management stations, such as an SNMP server, are connected to VLAN1.
  - VLANs 2-5 are user VLANs for devices such as user PCs.

Virtual Private Networks

- VPN’s enable an organization to use Public Networks such as the Internet, to provide a Secure connection among the organization’s wide area network.
- Customers can use VPN’s to connect an enterprise Intranet to a wide area network comprised of partners, customers, resellers and suppliers.
- Traditionally, businesses have relied on private 56-Kbps or T-1 leased lines to connect remote offices together.
- Leased lines are expensive to install and maintain
  - For small companies, the cost is just too high.
- Using the Internet as a backbone, a VPN can securely and cost effectively connect all of a companies offices, telecommuters, mobile workers, customers, partners and suppliers.
VPN Functionality

• A VPN needs to provide the following 4 critical functions:
  – Authentication – ensuring that the data originates at the source that it claims.
  – Access Control – restricting unauthorized users from the network.
  – Confidentiality – Preventing anyone from reading the data as it travels through the network
  – Data Integrity – Preventing anyone from tampering with the data as it traverses through the network

• Various approaches exist that offer authentication and access control for a VPN:
  – Challenge Handshake Authentication Protocol (CHAP)
  – Remote Authentication Dial-In Users (RADIUS)
  – Hardware-based tokens
  – Digital certificates

VPN Implementation Types

• Three Primary Forms:
  – A special purpose device consisting of a network interface, operating system and hardware based cryptographic support
  – A software solution that works with the OSI layers to provide encryption
  – A hybrid in which the VPN application runs on standard computing platforms that may use an outboard cryptographic processor
VPN Gateway and Tunnels

• A VPN gateway is a network device that provides encryption and authentication service to a multitude of hosts that connect to it.

• From the outside (Internet), all communications addressed to inside hosts flow through the gateway.

• There are 2 types of end point VPN tunnels:
  – Computer to Gateway
    • For remote access: generally set up for a remote user to connect to a corporate LAN.
  – Gateway to Gateway
    • This is the typical Enterprise-to-enterprise configuration. The 2 gateways communicate with each other.

VPN Protocols

• Four protocols have been suggested for creating VPNs.
  – Point to Point Tunneling Protocol (PPTP)
  – Layer 2 Forwarding (L2F)
  – Layer 2 Tunneling Protocol (L2TP)
  – IP Security Protocol (IPSec)

• The reason for so many choices is that for some corporations VPNs are used as their remote access security mechanism for others it is a secure tunnel between LANs.

• PPTP, L2F, and L2TP are used primarily for remote access, while IPSec is used for LAN to LAN tunneling.
Point to Point Tunneling Protocol (PPTP)

- PPTP originated from Microsoft’s secure remote access to capability with Windows NT.
- It is derivative of PPP (the popular dial-in point to point protocol).
- PPTP encapsulates PPP packets over a modified version of the Generic Routing Encapsulation (GRE) protocol
  - GRE is a protocol for facilitating the encapsulation of one protocol into another (RFC 1701 & 1702).
- PPTP relies on the PPP authentication procedure, password authentication and Challenge Handshake Authentication Protocol (CHAP).
- It does not support strong encryption and token-based authentication.

Layer 2 Forwarding (L2F)

- L2F is similar to PPTP and was developed around the same time period. It is also a remote access VPN technology.
- It is a layer 2 VPN implementation and can support other media like Frame relay and ATM.
- It is also based on PPP authentication but can also support Terminal Access Controller Access Control System (TACACS) and RADIUS for authentication.
- It supports multiple connections in one VPN tunnel through a connection ID tag.
- It supports 2 levels of authentication: one at the ISP level and another at the enterprise level.
Layer 2 Tunneling Protocol (L2TP)

- L2TP is an IETF standard (RFC 2661, 1999) designed as the next generation VPN protocol to replace PPTP & L2F.
- Also uses PPP through the Internet but defines its own tunneling protocol based on the work done by L2F.
  - It uses IPSec’s encryption algorithms.
- It includes the Password Authentication Protocol (PAP), CHAP authentication protocol, as well as RADIUS.

IPsec

- A protocol used to enhance IP with security.
- Establishes a simplex connection, known as Security Association (SA).
  - Unlike normal IP, that is connectionless.
  - It’s a simplex connection, so we’d need two SAs for a full-duplex secure connection.
- Provides Authentication Header (AH), and Encapsulating Security Payload (ESP).
- AH is used for authentication, ESP is used for: authentication and confidentiality.
- Used in transport mode (host-to-host), or tunnel mode (gateway-to-gateway).
IPsec AH

- The IPsec authentication header in transport mode for IPv4.

<table>
<thead>
<tr>
<th>IP header</th>
<th>AH</th>
<th>TCP header</th>
<th>Payload + padding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next header</td>
<td>Payload len</td>
<td>(Reserved)</td>
<td>Security parameters index</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sequence number</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Authentication data (HMAC)</td>
</tr>
</tbody>
</table>

**HMAC**: Hashed Message Authentication Code
Packet, and some IP header fields, are hashed together with a private key to form a “digital signature”.

- How to let the receiver know that this packet is an IPsec packet?
  - Set the *protocol* field in the IP header to be IPsec (value 51)

AH fields

- **Next Header**: the actual “protocol” field in the IP header that was replaced with 51.
- **Payload Length**: length of AH (in counts of 32-bits)
- **Security parameters index**: connection identifier, indicates the connection that this packet belongs to.
  - Each connection has its own key. Therefore the receiver knows, from this identifier, which key to use.
- **Sequence number**: used not for ordering (like TCP) but to prevent replay attacks!
  - Wrap-around is not allowed.
IPsec ESP

- Used for both authentication and confidentiality.
- ESP header has fields similar to the AH header, plus some more for encryption purposes.
- HMAC is a trailer (rather than a header) due to easier hardware implementation (like Ethernet’s CRC).

VPN Components

- There are four components to a VPN network.
  - The Internet
    - Fundamental plumbing for the network
  - Security Gateways
    - Sit between public and private networks preventing unauthorized intrusion (Firewalls, routers, integrated VPN hardware and software.)
    - May provide tunneling and encrypt private data.
  - Security Policy Servers
    - Maintains Access control lists that the security gateway uses to determine which traffic is authorized. For example some systems use a RADIUS server for these policies.
  - Certificate Authorities
    - These are used to confirm the authenticity of shared keys among sites. Companies might choose to maintain their own digital certificate server or might use an external agency of creating an extranet.

- Part of the challenge we face as network designers is to decide how much of this functionality should be integrated into one or more devices (firewalls, special purpose hardware, etc.).
Network Placement

• General Placement Rules
  – VPN Gateway must not be single point of failure
  – VPN Gateway must only accept encrypted traffic
  – VPN Gateway must accept encrypted and unencrypted traffic from the “trusted” network
  – VPN Gateway must defend itself from Internet threats

• Relation to the Firewall
  – In front of firewall
    • Single connection, that accepts encrypted and unencrypted traffic, you might not know if gateway was compromised from the Internet
  – Behind the firewall
    • Firewall will protect gateway, but opening must be made in the firewall for the gateway to function
  – On the firewall
    • A technological challenge (why?), starting to see more of this
  – VPN gateway on the firewall side (Currently the best solution)
    • Firewall outside connects to both the Gateway and the Internet
    • Gateway connects to the Internet, but only accepts encrypted traffic. Once gateway decrypts, information is filtered by firewall. All unencrypted traffic goes to the firewall.

Network Placement Details

The Gateway will only accept encrypted Traffic, after decryption, traffic flows through the firewall.
Performance

- Cryptographic processing is **computationally intensive**
  - Specially public key encryption used in authentication
  - Also, continuous encryption/decryption (e.g., secure video conferencing) requires constant high performance.
- General purpose computers typically do not have the proper I/O capability to perform the processing required at high performance.
- Thus, we have **Black Boxes** to provide the performance we need.
  - Typically dedicated hardware
- If QoS is important (e.g., Differentiated Services), you should separate your QoS requirements from your VPN requirements. Packets must be classified before the VPN encryption and the encrypted packets need to be marked for priority using IP Type of Service (ToS)