



**Press Release Contact Information:**

Thomas Cross  
TECHtionary.com  
CEO  
2525 Arapahoe Suite E-4  
Boulder, Colorado  
80302  
Voice: 303-444-6226  
E-Mail: [Email us Here](mailto:info@techtionary.com)  
Website: [Visit Our Website](http://www.techtionary.com)

**TECHtionary.com TECH-Tips - Week of June 20-24 - SIP - WiFi-QoS - Server Security - HSRP-Hot Standby - Fiber Channel**

*The following are the animated TECH-Tips for the week of June 20-24.*

**/24-7PressRelease/** - Boulder, CO, June 18, 2005 - Monday TECHtionary.com TECH-Tip - SIP-Session Initiation Protocol Proxy Server

The animated TECH-Tip tutorial available at <http://www.techtionary.com>

**Summary**

SIP-Session Initiation Protocol is the real-time communication protocol for VOIP-Voice over IP. SIP has been expanded to support video and instant-messaging applications.

**Details**

SIP is designed to perform basic call-control tasks, such as session call set up and tear down and signaling for features such as call hold, caller ID, conferencing and call transferring. However with SIP, the intelligence for call setup and features resides on the SIP device or user agent, such as an IP phone or a PC with voice or instant-messaging software. In contrast, traditional telephony or H.323-based telephony uses a model of intelligent, centralized phone switches with dumb phones with SS7-Signaling System 7 in PSTN-Public Switched Telephone Network telephone switching and H.323 or Media Gateway Control Protocol in IP telephony providing call control/routing. For more go to [www.sipforum.org](http://www.sipforum.org)

SIP-Session Initiation Protocol Proxy Server Forks (select different paths) Invite(s) to multiple User Agents (telephones). Forks can be sequential or concurrent. Session established to first UA-User Agent to respond with OK. Cancel sent to non-respondent (no answer) User Agents. Forks are useful in a call center environment or call hunting. Proxy Server call flow is where Proxy Server sets up call. Proxy Server is an optional SIP-Session Initiation Protocol component that handles routing of SIP signaling but does not initiate SIP messages. SIP call flow with Redirect Server. Redirect Server an optional SIP component that does not route SIP messages. Redirect Server returns a redirect (change in routing) to UA-User Agent for direct routing (SIP is designed for end-to-end signaling without intervention by a server). Shown is an example of SIP-Session Initiation Protocol used for instant messaging. The function of a Presence Server is to manage access, connections, directory (who's who), billing and tracking and other management functions. Here is an example of SIP-Session Initiation Protocol used for enhanced, multi-user, multi-media conferencing. Note internet access or VXML-Voice eXtensible Markup Language applications can be directed based on an Exception-triggered instant conference such as a disaster.

-----

Tuesday TECHtionary.com TECH-Tip -WiFi - QOS-Quality of Service

The animated TECH-Tip is available at <http://www.techtionary.com>

**Summary**

WiFi QoS solutions provide for real-time management control restricting users from access to specific applications or servers or the internet. At the same time, guest users can have access to public reception, registration conference rooms or supplier access areas such as the dock, storerooms, etc.

**Details**

Many WiFi networks are open access, unlimited user network without control restrictions, security or management accounting control. SSID-Service Set Identifier is a 32-character unique name attached to the header of packets sent over a WLAN-Wireless Local Area Network that acts as a password when a mobile device tries to connect to the AP-Access Point. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A SSID is required to gain access to the AP. Because an SSID can be sniffed (monitored and stolen) from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name as it is a name that identifies a wireless network. There are solutions that provide for real-time management control restricting users from access specific AP-Access Points at specific times. These devices can prioritize by user, group or application allowing bandwidth to be optimally allocated always while providing real-time monitoring of AAA-Authorization, Authentication and Accounting services. WiFi-QoS solutions provide for real-time management control restricting users to access specific AP-Access Points at specific times for time of day restrictions (work shift access) as well as nights and weekends. WiFi QoS solutions provide for real-time management control restricting users from access to specific

applications or servers or the internet. At the same time, guest users can have access to public reception, registration conference rooms or supplier access areas such as the dock, storerooms, etc.

-----

Wednesday TECHtionary.com TECH-Tip - Server Security

The animated TECH-Tip tutorial is available at <http://www.techtionary.com>

Summary

Server security may be the most important means of "risk management." That is, the majority of computer crime comes internally from disgruntled or dishonest employees. Even unintentional mistakes from undisciplined or untrained staff represent a major source of computer problems.

Details

Tactical - Server security control used in conjunction with router and firewall security policy adds internal controls. This tutorial is not about pass/phrase word management but on server security controls which can, among other things:

1-Block access to all in/outbound TCP-Transmission Control Protocol and UDP-User Datagram Protocol ports - Before you can 1-Block access to all in/outbound TCP-Transmission Control Protocol and UDP-User Datagram Protocol ports, you need to understand TCP/UDP ports. This is a self-repeating animation to answer how TCP-Transmission Control Protocol Port Level Security and TLS-Transport Layer Security function. Block access to all in/outbound TCP ports also means to review all internal port access privileges. That is, if the server is NOT connected to the web, then disable FTP, telnet and other TCP port functions (depending on business rules).

2-Allow only network traffic from LAN servers (that is, certain ports are only used with servers having internet access) -

Allow only network traffic from LAN servers - suggests that network traffic to backup or mirror (duplicate) servers should be monitored to ensure backup data is not compromised or corrupted.

3-Limit traffic between internal servers and users and 4-Enforce domain membership are both issues related to internal organizational structure and rules related to how networks are maintained. That is, traffic policies have descending and ascending relationships. Often higher rules control all devices and users below them. Conversely certain rules are only controlled at the lowest level. For more information on this subject contact your server software supplier.

----

Thursday TECHtionary.com TECH-Tip - HSRP-Hot Standby Routing Protocol and Proxy ARP-Address Resolution Protocol

The animated TECH-Tip tutorial is available at <http://www.techtionary.com>

Summary

HSRP is a Cisco protocol designed to provide automatic or standby router services in the case of disaster or failure.

Details

Phantom routers can exist throughout a network. The MAC-Media Access Control address and the IP-Internet Protocol addresses are passed among routers. This creates a virtual router called a Phantom router. It works like this:

- One router is designated as the Active router and the other as the Phantom/Standby router. The Active router routes packets for the Phantom/Standby router.

- Route Table/List updates are sent via HSRP-Hot Standby Routing Protocol via Hello messages.

- If the Phantom/Standby router does not receive Hello packets, it assumes that the Active router has failed and begins routing packets. Shown is the HSRP packet format. As you can see above is the HELLO message operation code to provide status/update to the Phantom router. Proxy ARP-Address Resolution Protocol is the default feature on Cisco routers. This is a simple means of creating fault-tolerant networks with one or more additional routers. Each router can respond to user/workstation requests if the router can reach (send/receive) the IP-Internet Protocol address. Each workstation can dynamically access multiple routers from the LAN-Local Area Network. If any router fails, the workstation can immediately access other routers on the internetwork (network). Users can access this feature by changing their Windows setting default gateway. MHSRP is for multi-group (router) HSRP.

Friday TECHtionary.com TECH-Tip - FC-Fibre Channel protocol - Point-to-Point, Arbitrated Loop and Fabric.

The animated tutorial is available at <http://www.techtionary.com>

Summary

According to Alcatel, "The term switching fabric comes from the idea of criss-crossing logical pathways between ports in a switch or other similar network architectures. When every port has an independent link to every other port, the graphical depiction of such a configuration looks like woven fabric, thus the term switching fabric. The term has taken on a life of its own since it was coined and in general is a logical discussion of how the hardware in a switch, router, etc. passes information between the ports."

Details

In the FC-Fibre Channel protocol, three different fabric topologies: 1-Point-to-Point, 2-Arbitrated Loop and 3-Fabric.

1- PP or PTP-Point-To-Point topology (shown here) is a direct connection between two N\_Ports, with at least one of the ports being a server (initiator). The topology requires no arbitration (contention-sharing) for the storage media because of separate links/circuits for transmission and reception. However, the topology is limited to two nodes making it not scalable.

2 - There are two types of FC-Fiber Channel AL-Arbitrated Loop: 1-Hub to interconnect the ports and 2-Daisy-Chain the devices. Arbitrated Loop combines the advantages of the fabric topology (support for multiple devices) with the ease-of-operation of point-to-point topology. In a FC-AL topology, devices are connected to a central hub. Like Ethernet LAN-Local Area Network Hubs, the Hub arbitrates (shares) access to devices and offers no additional functionality or intelligence to the

connected devices beyond serving as a centralized connection point.

In an Arbitrated Loop Hub, devices must seize control of the loop (carrier sense) and then establish a point-to-point connection with the receiving device. Once the point-to-point connection is established data is transferred. Once the transmissions have ended, devices connected by the Hub can once again "arbitrate" (share-contend) to gain control of the loop for establishing subsequent point-to-point connections. In Hub topology, there can be up to 126 nodes connected to a single link though with contention access the more the devices on network, the lower the performance. This makes is highly uncommon to attach the 126-node maximum to a single link.

In an FC-AL-Fibre Channel-Arbitrated Loop Daisy-chain, the devices are connected in a series and the transmit (send port) of one device is connected to the receive port of the next device in the chain. Daisy-chain networks are ideal for small networks but not very scalable since all devices on the loop are must be operational (on) at the same time for the loop to be up and running. The failure of a single device will cause a break to the loop, and cause the entire loop to cease operation.

3 - Fabric topology consists of one or more Fibre Channel switches interconnected through one or more ports. The fabric ports are X Ports that connect to either another X Port on a different switch or to an Y Port on a node. Each switch typically contains 8, 16, 32 or 64 ports; the two largest types are sometimes called director switches.

About <http://www.techtionary.com> - 303-444-6226

TECHtionary Corporation founded in 2001 and headquartered in Boulder, Colorado is the World's First and Largest Visualized Animated (rich media) Library/Magazine on Technology. Get the analysis and more than 2,575+ FREE tutorials on data, internet, wireless, VoIP-Voice over Internet Protocol (IPT-Internet Telephony Protocol), PBX systems, central office switching, protocols, telephony, telecommunications, networking, routing, power systems, broadband, WiFi-Wireless Fidelity and other technologies, TECHtionary.com provides "just enough - just-in-time" critical success information. TECHtionary produces web infomercials proven to "increase revenues, decrease customer support costs and increase customer satisfaction."