# Protecting Enterprise Extender Traffic with a VPN

Section 9913
August 09,2011
STG Lab Services

Thomas Cosenza, CISSP
tcosenza@us.ibm.com

# Agenda

- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

# Why Add Security

- ID theft is on the rise
- Meet new standards
  - PCI standard
  - HIPPA
  - SOX
  - European Common Standard
  - US regulations starting to come around
    - *California SB 1386*
- Keep the business out of the paper

# Why Add Security

- Failure to Secure your business
  - Fines and penalties
  - Incidents from loss of  credit card holder data
    - *Costs for forensics examinations*
    - *Liability*
    - *Dispute resolution costs*
  - Stock Shares plummet
  - Loss of Customers

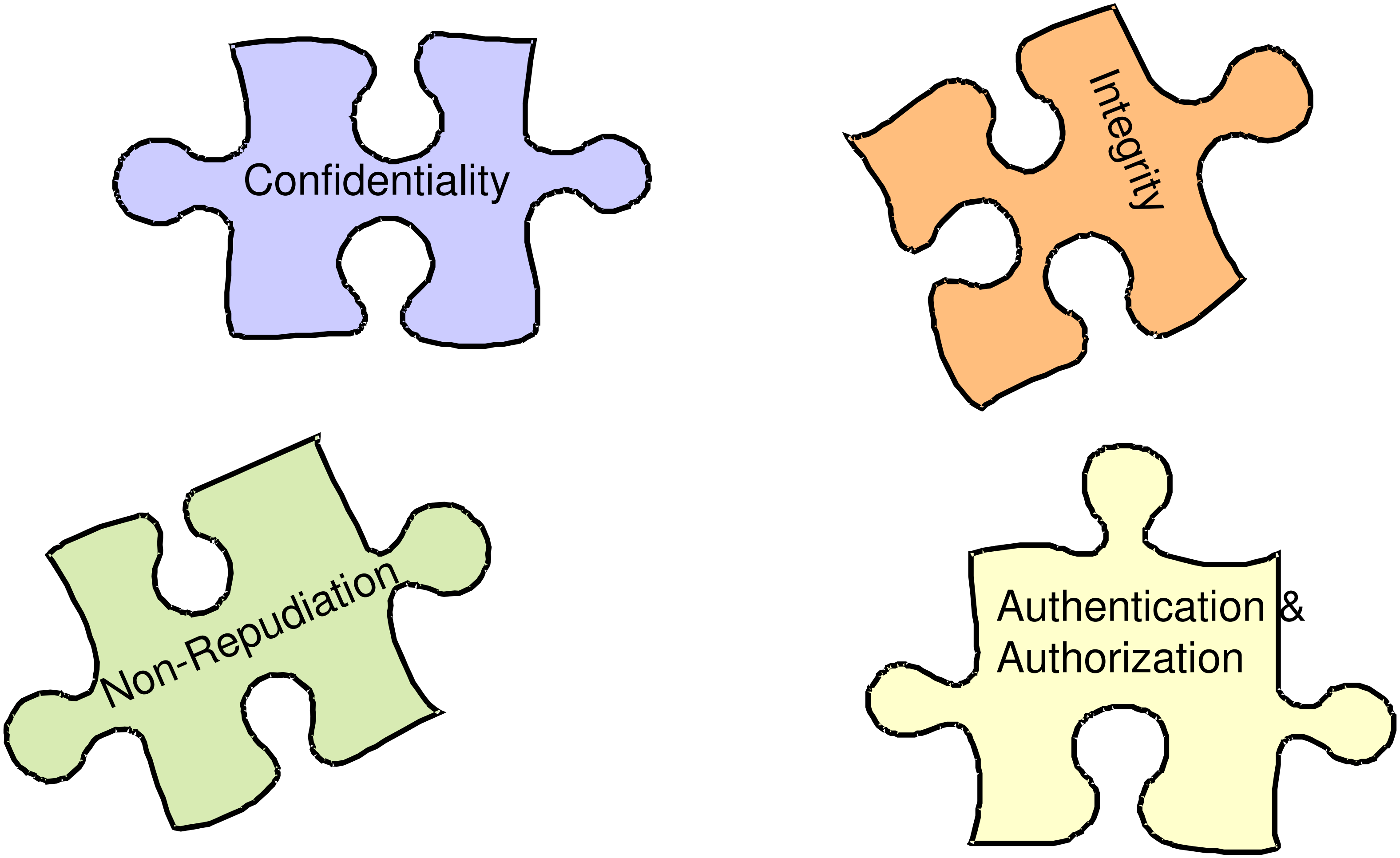
# Words to Live By

- “The Security Perimeter is now at the End Point” Anonymous

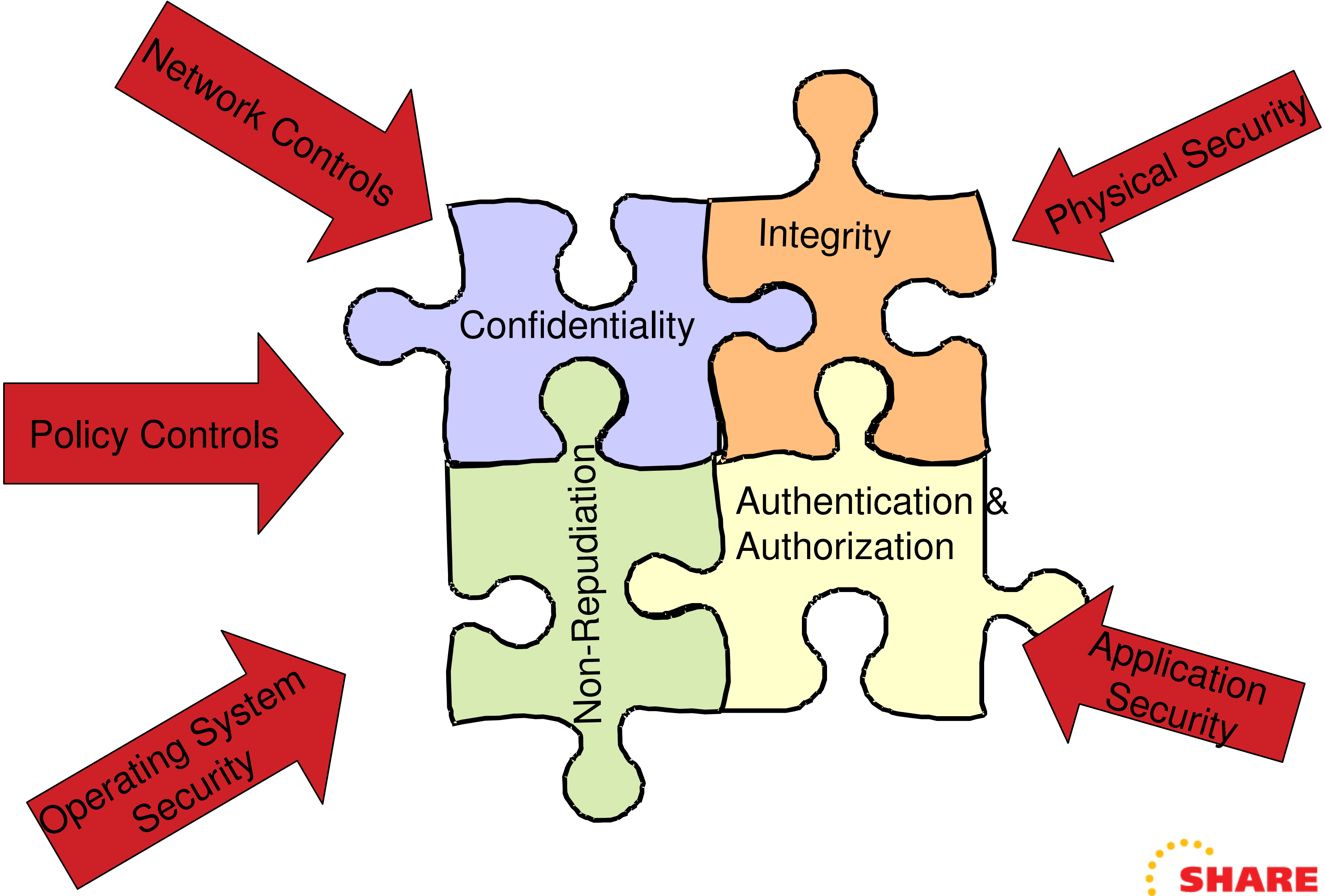
# Agenda

- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

# The Puzzle pieces of Security



# Putting the Pieces Together



# How Does EE Measure UP

- Authorization
  - OS control of datasets
- Access Control
  - APPN Topology Definitions
- Data Confidentiality
  - Session Level Encryption (static keys)
- Data Integrity
  - Checksums
- Non-Repudiation
  - None

More is needed!!!!

# EE with VPN

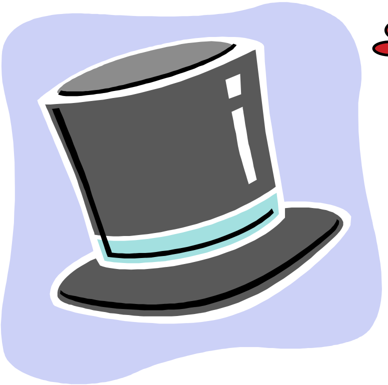
- Authorization
  - EE Traffic can be authenticated with x.509 Certificates
- Access Control
  - Have to have the properly negotiated keys
- Data Confidentiality
  - Can Take advantage of  AES or Triple DES encryption and Dynamic Key creation
- Data Integrity
  - IPSec has built in integrity checks
- Non-Repudiation
  - If you are using “End to End” VPNs the certificate you negotiate with had to come from a known party

# Agenda

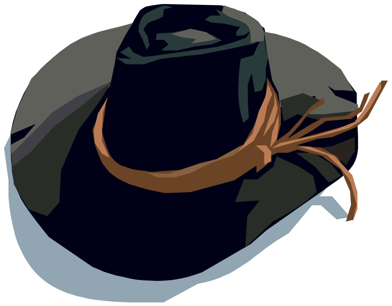
- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

# HATS

SNA: It's an Interface



Enterprise Extender



IP: It's an Application

## Modeling the EE traffic with my IP Hat

- What is EE from an IP Perspective
  - Uses UDP
  - Ports 12000 – 12004
    - 12000 – Signaling
    - 12001 – EE Network Flow Control
    - 12002 – High Priority Traffic
    - 12003 – Medium Priority Traffic
    - 12004 – Low Priority Traffic
  - Using Static VIPA Addresses

# Agenda

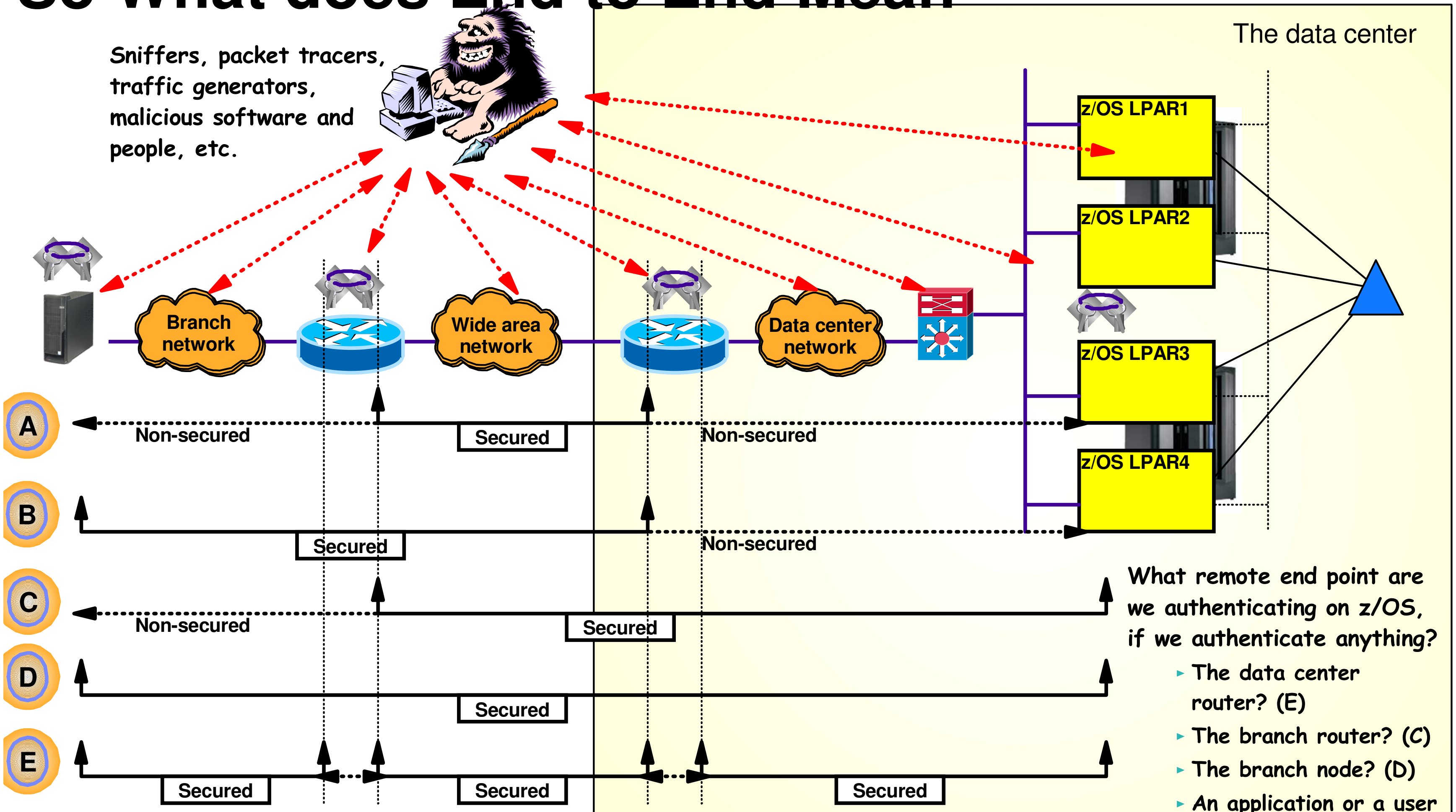
- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

# IPSec Overview

- Increasing the Network Security Layer
- Created for IPv6
- Adopted for IPv4
- Dynamic Key Exchange
    - Internet Key Exchange (IKE)  – Uses UDP 500
    - Two phases to this
- Available on most platforms
- Two Protocols
    - AH
    - ESP
- Two modes
    - Tunnel Mode
    - Transport – Can only be used in end to end case

# So What does End to End Mean

Sniffers, packet tracers, traffic generators, malicious software and people, etc.



What remote end point are we authenticating on z/OS, if we authenticate anything?

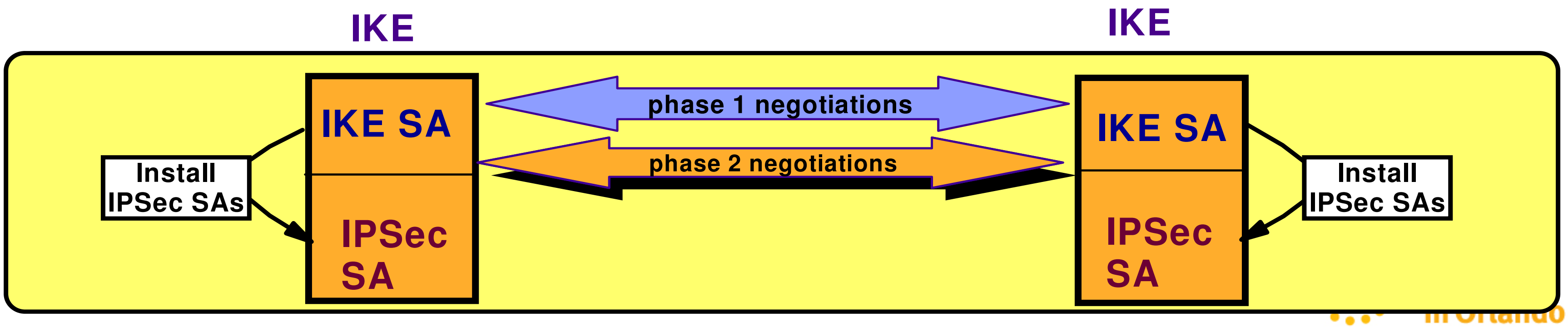
- The data center router? (E)
- The branch router? (C)
- The branch node? (D)
- An application or a user on the branch node? (D if connection-level security is used)

Only option D provides ultimate end point authentication, end-to-end confidentiality, and end-to-end message integrity.

# Break down of VPN

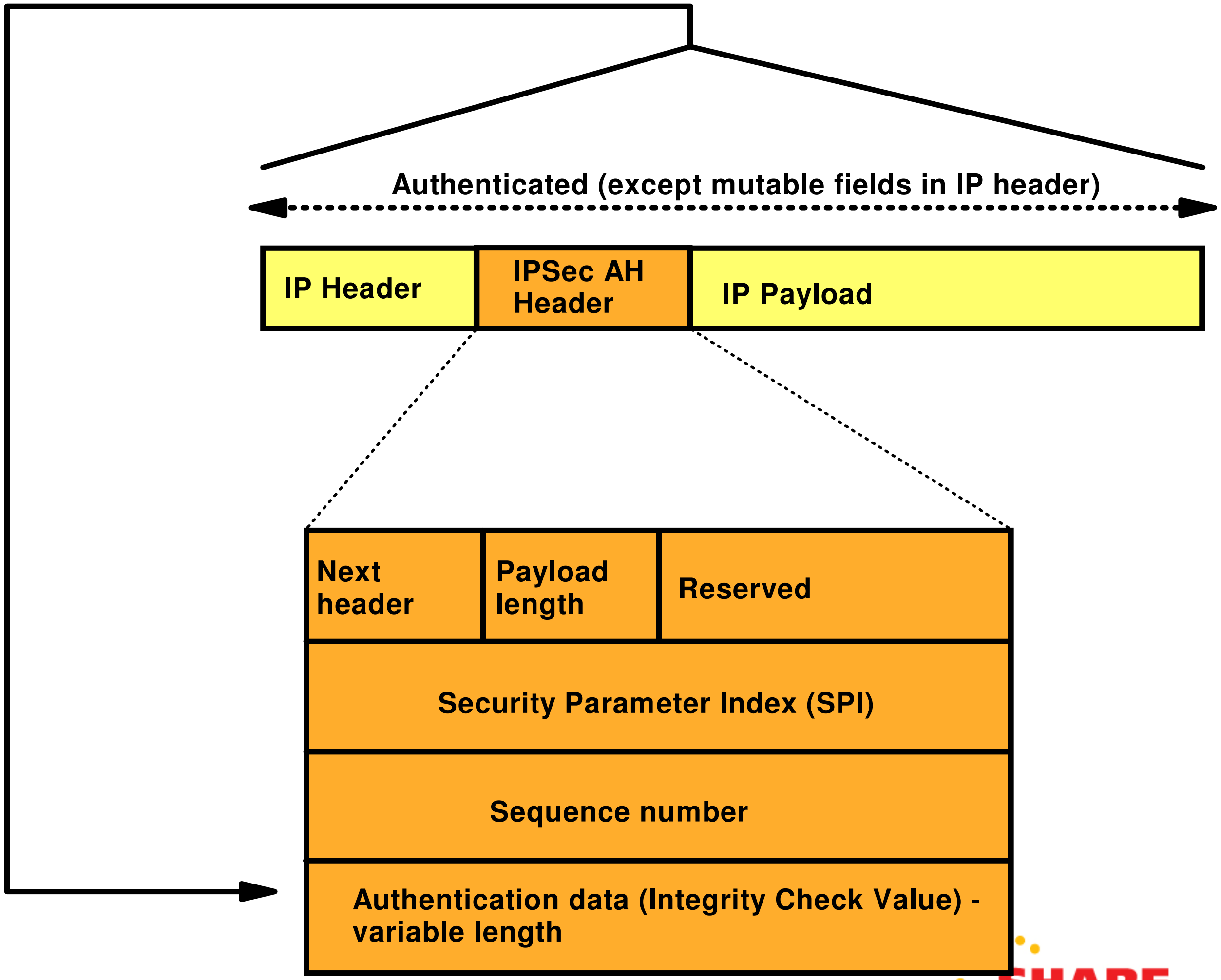
- **Phase 1 negotiation**
  - Creates a secure channel with a remote security endpoint
    - Negotiates an IKE SA
      - Generates cryptographic keys that will be used to protect Phase 2 negotiations and Informational exchanges
      - Authenticates the identity of the parties involved
      - Bidirectional, and not identified via SPIs
  - Requires processor-intensive cryptographic operations
  - Done infrequently

- **Phase 2 negotiation**
  - Negotiates a pair of IPSec SAs with a remote security endpoint
    - Generates cryptographic keys that are used to protect data
      - Authentication keys for use with AH
      - Authentication and/or encryption keys for use with ESP
  - Performed under the protection of an IKE SA
  - Done more frequently than phase 1



# Make up of an Authentication Header packet (AH)

IP Protocol number 51

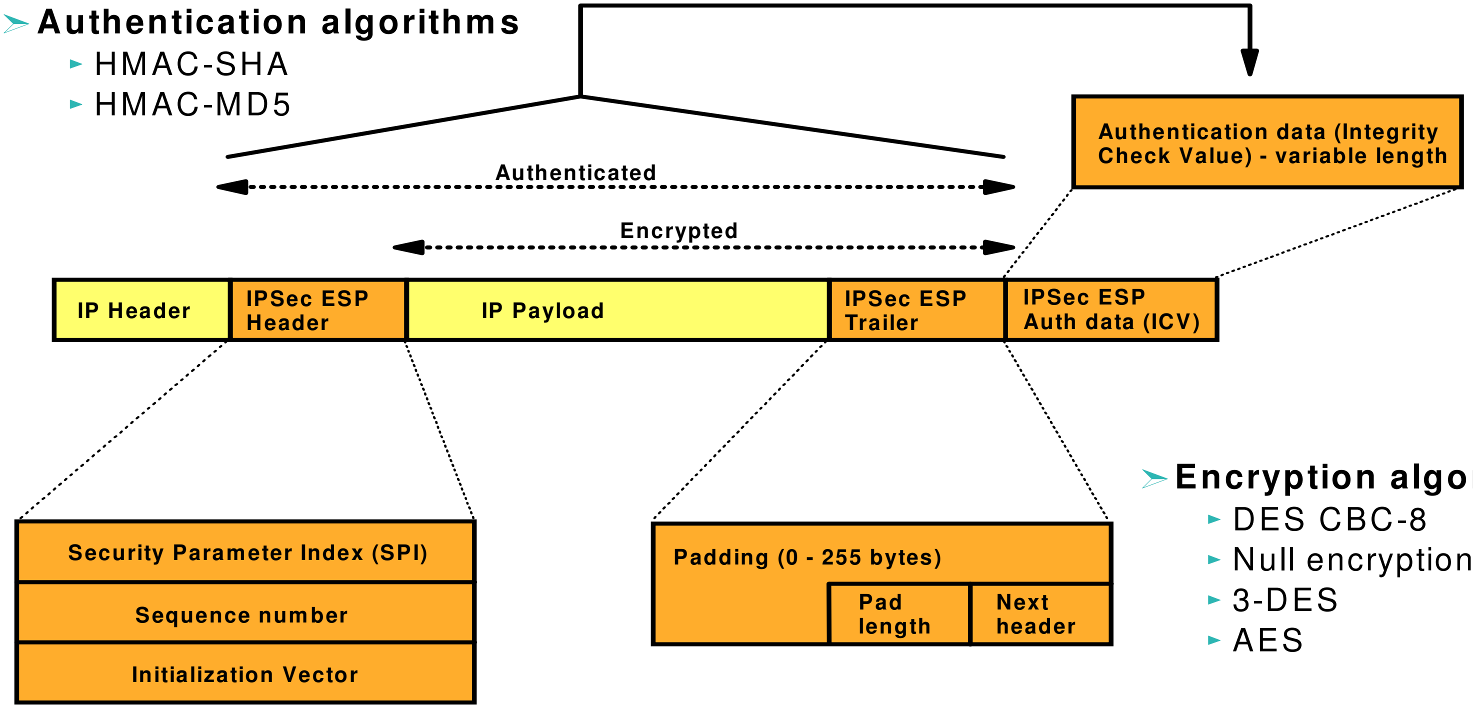

Authenticated (except mutable fields in IP header)
IP Header
IPSec AH Header
IP Payload
Next header
Payload length
Reserved
Security Parameter Index (SPI)
Sequence number
Authentication data (Integrity Check Value) - variable length

- **Authentication algorithms**
  - HMAC-SHA
  - HMAC-MD5

# Make up of an Encapsulated Security Payload (ESP)

IP Protocol number 50

- Authentication algorithms
  - HMAC-SHA
  - HMAC-MD5



Authenticated

Encrypted

Authentication data (Integrity Check Value) - variable length

| IP Header | IPSec ESP Header | IP Payload | IPSec ESP Trailer | IPSec ESP Auth data (ICV) |
|---|---|---|---|---|

Security Parameter Index (SPI)

Sequence number

Initialization Vector

Padding (0 - 255 bytes)

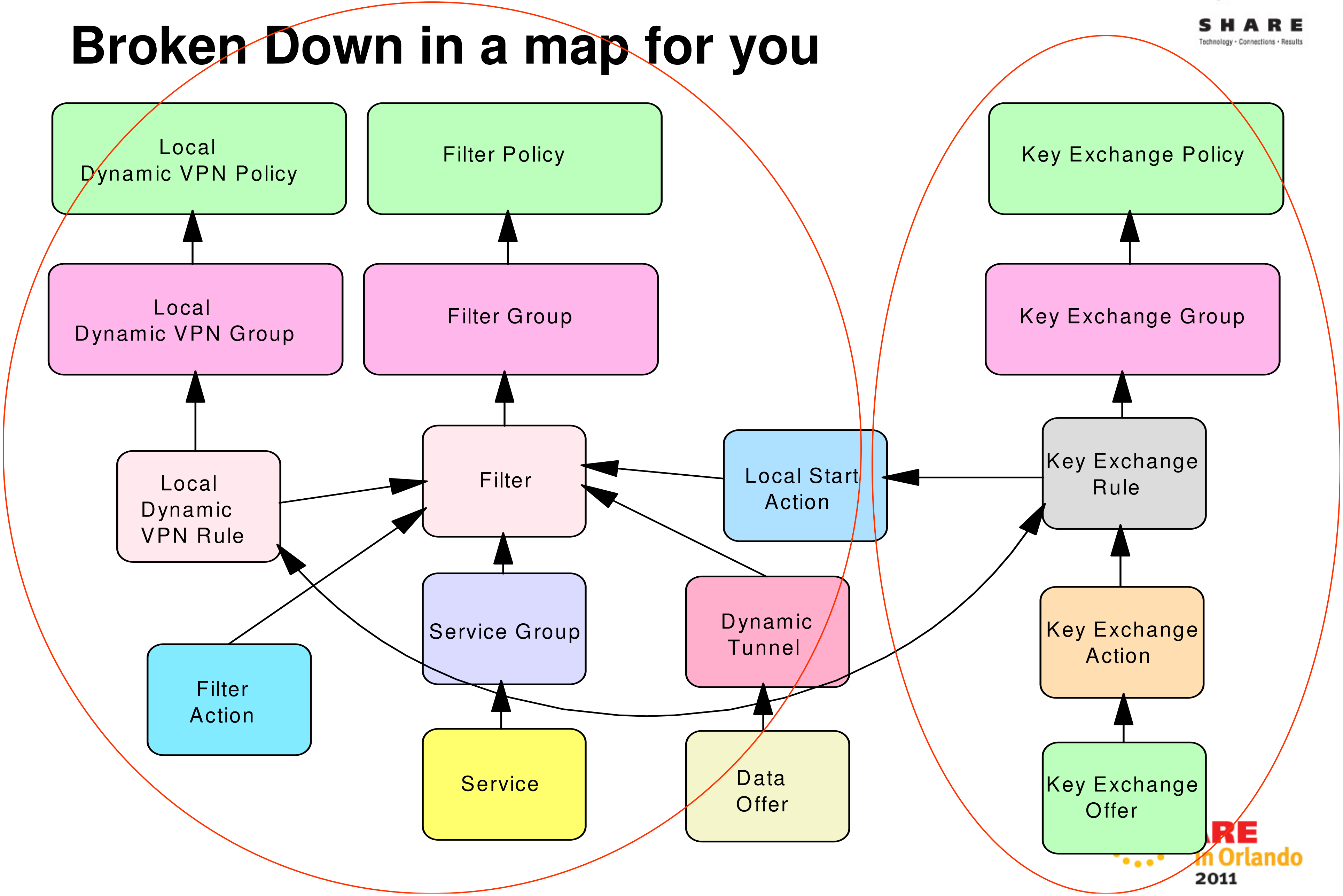
Pad length

Next header

- Encryption algorithms
  - DES CBC-8
  - Null encryption
  - 3-DES
  - AES

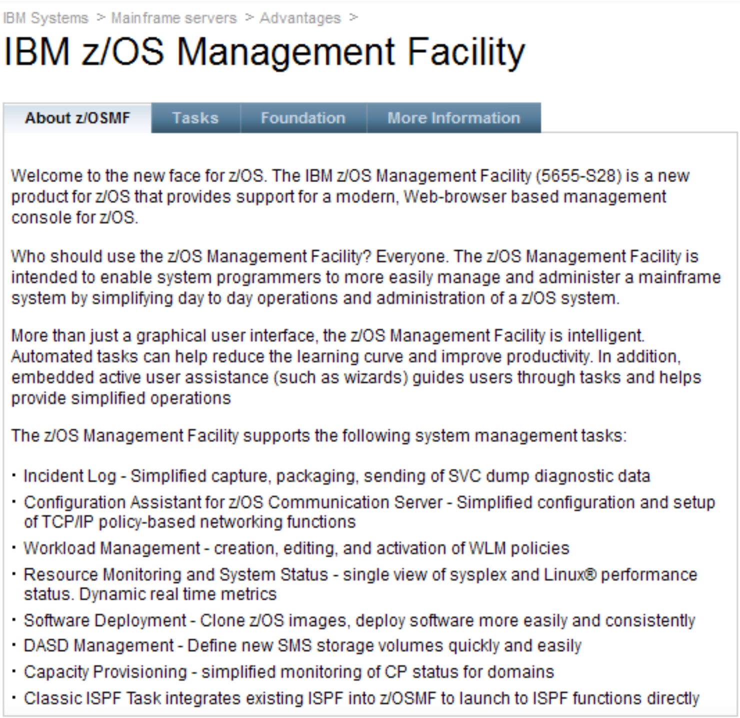
- If transport mode, then "Payload" contains the original transport header and original data (possibly encrypted)
- If tunnel mode, then "Payload" contains original IP header, original transport header, and original data
  - "Payload" can be encrypted

# Broken Down in a map for you



# Tip for IPSEC

- IBM Configuration Assistant for z/OS – Current all releases
- zOSMF for V1R12 and higher



## IBM z/OS Management Facility

Welcome to the new face for z/OS. The IBM z/OS Management Facility (5655-S28) is a new product for z/OS that provides support for a modern, Web-browser based management console for z/OS.

Who should use the z/OS Management Facility? Everyone. The z/OS Management Facility is intended to enable system programmers to more easily manage and administer a mainframe system by simplifying day to day operations and administration of a z/OS system.

More than just a graphical user interface, the z/OS Management Facility is intelligent. Automated tasks can help reduce the learning curve and improve productivity. In addition, embedded active user assistance (such as wizards) guides users through tasks and helps provide simplified operations

The z/OS Management Facility supports the following system management tasks:

- Incident Log - Simplified capture, packaging, sending of SVC dump diagnostic data
- Configuration Assistant for z/OS Communication Server - Simplified configuration and setup of TCP/IP policy-based networking functions
- Workload Management - creation, editing, and activation of WLM policies
- Resource Monitoring and System Status - single view of sysplex and Linux® performance status. Dynamic real time metrics
- Software Deployment - Clone z/OS images, deploy software more easily and consistently
- DASD Management - Define new SMS storage volumes quickly and easily
- Capacity Provisioning - simplified monitoring of CP status for domains
- Classic ISPF Task integrates existing ISPF into z/OSMF to launch to ISPF functions directly

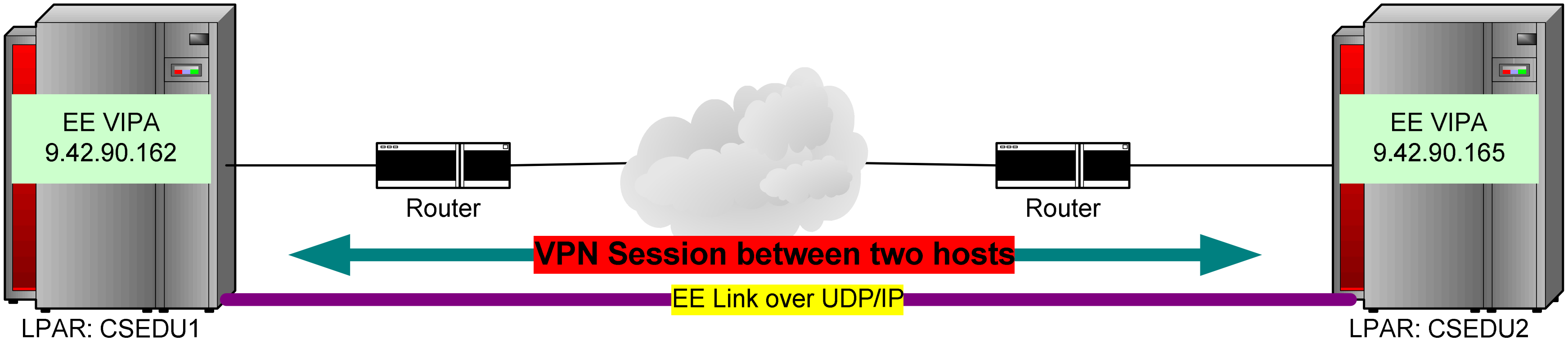
# Agenda

- Reasons for Security
- Overview of Security
- Overview of VPN
- Modeling EE Traffic
- Demo of EE over VPN

# Some preparation needed

- IPCONFIG IPSECURITY (Replace IPCONFIG FIREWALL)
- POLICY AGENT SETUP
- EE Deck Creation
  - XCA
  - SMN

# Overview of the Demo



# The Demo!!!

# Useful commands

- D NET,EE
- D NET,EE,IPADDR=static Vipa
- D NET,EEDIAG
- D TCPIP,<stack>,n,config
- ipsec –y display <–r wide>
- ipsec –k display

# This Demo is on the Web

- This demo from beginning to end will be available for you to watch on the web

Communication Server Security Site

http://www-306.ibm.com/software/network/commserver/zos/security/

Direct Link

http://www.ibm.com/support/docview.wss?rs=852&uid=swg27013261

# IMPORTANT !!!!!!!!!!

- Improved performance for EE over IPSec
  - The “bursty” nature of HPR traffic can cause significant performance degradation when it is carried over IPSec tunnels
  - Smaller bursts frequently get encrypted and sent before larger bursts. This results in out-of-order segments that are dropped at the other end of the IPSec tunnel, forcing retransmits.
  - V1R11 breaks large bursts into batches of smaller bursts
  - PTFed back to V1R10 – APAR PK93190
- Improved support for EE over IPSec when IPSec processing offloaded to a zIIP
  - Support for offloading outbound EE over IPSec traffic to a zIIP processor. Previously only inbound traffic was processed on the zIIP
  - V1R11 only

# Questions?

IBM

**Thomas Cosenza**

*System z I/T Specialist*

*IBM STG Lab Services*

*XI50z Team Lead*

*3031 N Rocky Point DR*
*Tampa, FL 33607-5878*

*Tel 720-395-7392*
*Mobile 813-270-9911*
*Email: tcosenza@us.ibm.com*

# For More Information....

| URL | Content |
|---|---|
| http://www.ibm.com/systems/z/ | IBM System z |
| http://www.ibm.com/systems/z/hardware/networking/index.html | IBM System z Networking |
| http://www.ibm.com/software/network/commserver/zos/ | IBM z/OS Communications Server |
| http://www.ibm.com/software/network/commserver/z_lin/ | IBM Communications Server for Linux on zSeries |
| http://www.ibm.com/software/network/ccl/ | IBM Communication Controller for Linux on System z |
| http://www.ibm.com/software/network/commserver/library | IBM Communications Server Library - white papers, product documentation, etc. |
| http://www.redbooks.ibm.com | IBM Redbooks |
| http://www.ibm.com/software/network/commserver/support | IBM Communications Server Technical Support |
| http://www.ibm.com/support/techdocs/ | Technical Support Documentation (techdocs, flashes, presentations, white papers, etc.) |
| http://www.rfc-editor.org/rfcsearch.html | Request For Comments (RFCs) |
| http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp | IBM Education Assistant |