Plamen Nedeltchev
Ph.D. Sr. Member of Technical Staff, Cisco IT

Bob Scarbrough
IT Program Manager, Cisco IT, (Host)
RAEX Agenda

ACCESS MARKET CHALLENGES AND DEMANDS.
RAEX PROGRAM AND ITS COMPONENTS.
TOTAL COST OF OWNERSHIP (TCO)

NG ECT NETWORK AS A PLATFORM:
End to end VPN model and TCO
End to End Security
End to End Connectivity
End to End Provisioning with Cisco Security Manager (CSM)
End to End Deployment with Cisco Security Manager (CSM)
End to End Management with Cisco Security Manager (CSM)

SERVICE ORIENTED ARCHITECTURE OVER VPN.
QOS, IP SLA and Lessons learned
Enterprise Class Teleworker (ECT)

Residential BRODBAND penetration

VPN Technologies of Cisco.

IP Phone
Cisco 8XX Router
Broadband Internet
Encrypted VPN Tunnel
VPN Head-end Router
Corporate Network

Data
Wi-Fi
Voice
Video

Enterprise Class Services – encrypted data, IPT, video, WIFI

Full office replica Near office or equal office user experience..

ZTD, Automated Management, manageable TCO.
The Telecommunication industry transition and the broadband explosion.

- Industry’s transitioning from permanent circuits to broadband connections is finally gaining speed. The lead times for permanent circuits for sales offices in the emerging markets continue to be between 3 months and 9 months. The pricing in some cases is a showstopper.

- The residential broadband offerings are ranging from typical 1.5 Mbps for DSL to 6 Mbps for Cable. Some providers offer FTTH to the home and it is expected most of the ISP providers to reach 15-25 Mbps in the next 2 years on the access layers of their networks.
The Telecommunication industry transition and the broadband explosion. (Contd.)

- Telecommuting lifestyle is expected to continue to grow to up to 50 million people by Y2008. Internet over broadband continue to be a hostile environment as 70% of attacks are coming across Internet. Telecommuting as a trend is not only about productivity and business resiliency. It is about adding another dimension of freedom for the employees to better balance their personal live and business.

- Based on statistics provided by the OECD, published this year, in Y2006, the number of broadband subscribers globally has increased 26% from 157 million in December 2005 to 197 million in December 2006.

  SOURCE - Organization for Economic Co-operation and Development; www.oecd.org/sti/ict/broadband
The RAEX model is applicable for Telecommuter’s office, Branch, SMB, Commercial networking

- **Next Generation ECT** - provides the platform for Enterprise class services for home users and home offices. It addresses the needs of full time telecommutes, part time telecommuters and day extenders.

- **Site to site VPN over broadband** provides the framework for the next generation Site to site VPN. The point to point connections are not longer the only option Branch to Branch connectivity.

- **Teleworker QoS** ("Enabling "Guaranteed Internet"). By partnering with ISP, NG ECT will create a demand for differentiated services and it will allow the ISPs to offer them for their customers on the Access Layer of their network.

- **Business resiliency management.** NG ECT is positioned as one of the major Cisco technologies for crisis management and business continuity management.
NG ECT Solution
Cisco IOS-Based Site-to-Site VPN

- Enterprise, SMB or ISP models
- Spoke router in home network has two or three VPN tunnels; two data and one mgmt
- Traffic is routed over data tunnels in fail-over model
- Management subnet is separate from data subnet and can be geographically isolated
Cisco 870 Series Integrated Services Router

WAN Port:
871 = 100 MB Ethernet
876 = ADSL over ISDN
877 = ADSL
878 = G.SHDSL (4-wire)

Dual, Removable Antennae
ISDN S/T Port (876 and 878 Only)
Security Cable Lock

Trust Pool
10.25.224.16/28

Non-trusted Pool
10.0.2.0/24

4-Port 10/100 Managed Switch

WAN Port:
Reset

Memory
Flash
Default: 24 MB
Max: 52 MB

DRAM
Default: 128 MB
Max: 256 MB

Console Port/Virtual AUX Port
NG ECT is the RAEX enabler.

Cisco IT Deployment
- 5 Management Hubs,
- 11 pairs of Data Hubs.
Expected number of users – 30,000 +.
Site-to-Site VPN over Broadband

A Fully Integrated, Flexible and Secure Cisco Enterprise Branch Architecture extends Headquarter Applications in real-time to remote sites.

It allows the secure ECT architecture to integrate the security with Unified Communications and Mobility solutions under the centralized management:

- It reduces provisioning lead times.
- It allows jump start of the branch offices and faster penetration into emerging markets.
- It allows significant WAN cost and OPEX reduction.
- Reduces the dependency on ISP.
Enabling "Guaranteed Internet": The service is as good as its weakest link

For this traffic, the QoS marking will be honored and/or the traffic will be contention free.
## Communications Requirements for Business Resiliency Management

### Solution Suite

<table>
<thead>
<tr>
<th>Enabling Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Anywhere Office</strong></td>
</tr>
<tr>
<td><strong>Cisco ECT</strong></td>
</tr>
<tr>
<td><strong>VPN, VoIP, Conferencing</strong></td>
</tr>
</tbody>
</table>

### Communications Services

<table>
<thead>
<tr>
<th>Data Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Voice &amp; Data Connectivity</strong></td>
</tr>
<tr>
<td><strong>Best effort services</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full Office Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UC and collaboration tools</strong></td>
</tr>
<tr>
<td><strong>for key executives, decision makers and business critical resources.</strong></td>
</tr>
</tbody>
</table>
VPN solutions have evolved from business convenience to business critical, from technology to service, from remote access solution to remote UC.

- The future of RAEX will be about equal user experience, building new business models, deploying next generation services and Cisco gear, enabling mobility and presence; Unified communications and Collaboration.

- The Next generation ECT (part of RAEX) is making the next step up, building the service oriented network. It provides not only VPN access over the public networks for the remote users, but adds Enterprise class quality for data, voice, wireless and video. Besides, NG ECT offers an IP SLA to Cisco users and metrics to assess the quality of the provided services.

- The first generation Enterprise Class Teleworker Solution build the remote network architecture and became a platform for the next generations. ECT has proven to be a big cost saver for Cisco IT and Cisco customers. From industry prospective, for the Enterprise Environments, ECT – like managed security solutions are the preferred ones vs. non managed solutions due to their specifics and advantages.
ECT Reduces TCO

Total Cost of Ownership (TCO) is the sum of acquisition costs, plus all the operational and support costs over the lifetime of an asset—generally 3–5 years; as TCO decreases, ROI improves.

Maintain a Low TCO by Using
- Lower costs of provisioning.
- Low cost of deployment.
  IT 12-14% savings for ZTD for CPE.
- Lower costs of management
- Utilizing reusable components
- Automation of routine operations
NG ECT Solution: End to End VPN Model and TCO
## NG ECT and End-to-End VPN Model and TCO

### E2EVPN

<table>
<thead>
<tr>
<th>End-to-end security</th>
<th>End-to-end connectivity</th>
<th>End-to-end deployment</th>
<th>End-to-end management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device and User Authentication and anti-theft protection</strong></td>
<td><strong>DMVPN</strong></td>
<td><strong>Cisco Security Manager (CSM)</strong></td>
<td><strong>Ongoing Management Cisco Security Manager (CSM) Cisco IE2100 based CNS Notification Engine</strong></td>
</tr>
<tr>
<td>- Secure RSA Lock Key</td>
<td>- Failover/Load-balancing/SLB</td>
<td>- CNS Configuration Engine</td>
<td>- CNS Configuration Engine</td>
</tr>
<tr>
<td>- Secure ARP-proxy</td>
<td>- Dynamic routing</td>
<td>- CNS Notification Engine</td>
<td>- CNS Notification Engine</td>
</tr>
<tr>
<td>- Auth-Proxy-</td>
<td>- Full – mesh and partial - mesh topologies.</td>
<td>- CNS Image engine</td>
<td>- CNS Image management engine</td>
</tr>
<tr>
<td>- AAA IEEE 802.1X-AAA.</td>
<td>- Hub-to-spoke and spoke-to-speke tunnels. Permanent and on-demand tunnels</td>
<td><strong>Automated Zero Touch Deployment (ZTD)</strong></td>
<td><strong>EMAN Framework Integration</strong></td>
</tr>
<tr>
<td>- IOS-Based PKI</td>
<td>- mGRE, IPSec, NHRP. Transport and Tunnel modes</td>
<td>- Bootstrap Configuration and PKI certificates (SDP)</td>
<td><strong>Automated user service application and entitlement</strong></td>
</tr>
<tr>
<td>- Certificate Server (CA&amp;RA, Sub-CS modes)</td>
<td>- Multiple DMVPN clouds per head-end router. Resiliency</td>
<td>- Off-line (CSM CA Proxy)</td>
<td><strong>Automated configuration/pre-configuration and audit</strong></td>
</tr>
<tr>
<td>- PKI-AAA Integration</td>
<td>- Full support of IP applications</td>
<td>- In-house (RA engineer)</td>
<td><strong>Automated image Management</strong></td>
</tr>
<tr>
<td>- Auto-enrolment</td>
<td>- Data</td>
<td><strong>Automated policy deployment, re-deployment and audit</strong></td>
<td><strong>Automated control, monitoring and security management</strong></td>
</tr>
<tr>
<td>- Multiple Trust Points</td>
<td>- VoIP</td>
<td></td>
<td><strong>Interactive/ Automated decision making and service termination</strong></td>
</tr>
<tr>
<td>- <strong>Underlying security features</strong></td>
<td>- QoS</td>
<td></td>
<td><strong>Automated event log management</strong></td>
</tr>
<tr>
<td>- IPSec (3DES or AES)</td>
<td>- Wi-Fi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Stateful Firewall</td>
<td>- Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- NBAR and IDS</td>
<td>- Video</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- DMVPN
- Cisco CNS 2100 Series Intelligence Engine:
  - CNS Configuration Engine
  - CNS Notification Engine
  - CNS Image engine
- Automated Zero Touch Deployment (ZTD)
  - Bootstrap Configuration and PKI certificates (SDP)
  - Off-line (CSM CA Proxy)
  - In-house (RA engineer)
- Automated policy deployment, re-deployment and audit
  - DMVPN/ IPSec
  - Firewall
  - QoS
  - NAT
  - NBAR
## End-to-End IOS Layered Security

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Key Loss Due to Password Recovery</td>
<td>Guards against unauthorized configuration changes</td>
</tr>
<tr>
<td>Secure RSA Private Key</td>
<td>Prevents VPN connection after theft</td>
</tr>
<tr>
<td>Secure ARP</td>
<td>Anti-spoofing of IP addresses assigned to devices</td>
</tr>
<tr>
<td>Authentication-Proxy</td>
<td>User-level authentication (layer 3)</td>
</tr>
<tr>
<td>802.1x</td>
<td>User-level authentication (layer 2)</td>
</tr>
<tr>
<td>Cisco IOS® PKI Support and PKI-AAA Integration</td>
<td>Secure, scalable solution enables quick addition and deletion of spoke routers utilizing existing AAA servers</td>
</tr>
<tr>
<td>Cisco IOS® Stateful Firewall (CBAC)</td>
<td>Maintains state info per application, will provide deep packet inspection and off-board URL filtering</td>
</tr>
<tr>
<td>Cisco IOS® IPS</td>
<td>Multiple signatures, will combine with CBAC to perform deep packet inspection with single lookup</td>
</tr>
<tr>
<td>Network Based Application Recognition (NBAR)</td>
<td>Addresses IP QoS classification requirements by classifying application-level protocols so that QoS policies can be applied.</td>
</tr>
</tbody>
</table>
RSA Key Loss Due to Password Recovery

- If someone attempts password recovery on the router, the RSA private key will become unusable.
- If the user tries to change the hostname of the router, the RSA private key is permanently deleted.

The Router Cannot Establish a VPN Session Using the Installed Certificates After Password Recovery.
Secure ARP

- When the spoke router assigns an IP address via DHCP, the entry is secured in the ARP table.
- Intruder cannot just clear the ARP cache and use the IP address to gain access to the Cisco network.

Secure ARP is an effective anti-spoofing mechanism; however, the best approach for all services would be to require device certificates.
Authentication Proxy

- Authentication proxy enables user authentication at layer 3 of the network stack; the user must authenticate in order to gain intranet access from laptops, workstations, and PCs; upon successful authentication, an access list will be then downloaded to the router from the AAA RADIUS servers to enforce corporate access policies.

- Authentication proxy can be implemented as a mechanism to prevent non-authorized users from accessing corporate network.

- User access to different areas of an intranet can be controlled via the group info on the RADIUS server or can be combined with NAC or user identity management systems.
IEEE port authentication - 802.1x

- IEEE 802.1x provides layer 2 port authentication of devices
- 2 VLANs on the spoke router
  - Trusted (corporate routable) VLAN
  - Non-trusted (home) VLAN
  - Devices that pass 802.1x authentication assigned to trusted VLAN
- 802.1x simplifies router configuration vs. authentication proxy
Cisco IOS Certificate Server PKI-AAA Integration

- Cisco IOS PKI solution provides the necessary encryption, confidentiality and non-repudiation feature set and addresses the MIM attack.
- IOS-CS supports CA, RA, and subCS server modes.
- It supports exportable and non-exportable keys, full backup, restore, and auto-enroll.
- IOS-CS permits storage of certificates on external databases or on local flash.
- Cisco IOS PKI-AAA integration eliminates the need to manage CRLs, which significantly simplifies the management of the existing ECT environment.
Cisco IOS Firewalls Features

- Cisco IOS provides a stateful firewall and CBAC (Context-Based Access Control)
- The firewall ACL will block any non-authorized access inbound attempts (from Internet)
- CBAC will open temporarily some application associated ports for the return traffic if the connections initiated from the inside. Upon expiration of the default timeouts and if there is no more interesting traffic, these ports will be closed.
- Apart from standard TCP and UDP, CBAC also supports protocols like SIP, SCCP, SMTP, FTP, and more
Network Based Application Recognition (NBAR)

- NBAR is an intelligent classification engine that recognizes applications including Web-based and client/server applications which dynamically assign TCP or UDP port numbers.

- In NG ECT, NBAR is used to match and remark the time sensitive traffic (IPT, video, IPC) at the ingress interface and queue and prioritize the traffic based on the this marking. In such way the NG ECT changes the status of this traffic from non-trusted to trusted and allows the time sensitive applications to be routed in the corporate network in a cohesive way with other time sensitive traffic.

- Mission critical application can be guaranteed bandwidth.

- Improves VPN performance by ensuring identifying mission-critical traffic before it is encrypted, allowing the network to apply appropriate QoS controls.
NG ECT Solution: End-to-End Connectivity
## End-to-End Connectivity

### Feature | Benefit
--- | ---
DMVPN Fundamentals | Dynamic Multipoint VPN based upon IPSec, NHRP, and Multipoint GRE
Routing with DMVPN | Routing protocols in DMVPN cloud provide responsive failover
DMVPN Key Differentiators | Simplifies configurations, separates management and data traffic paths and builds on-demand full or partially meshed networks
Server Load Balancing (SLB) Overall design | The next generation DMVPN networks
DMVPN and SLB design | Server Load Balancing (SLB) design of DMVPN is an enhancement of DMVPN and can be delivered in two separate designs.
SLB DMVPN – Key Advantages | SLB is much easier to configure and support, scales higher, provides higher tunnel creation rate, and better redundancy.
DMVPN Fundamentals

Dynamic Multipoint VPN (DMVPN) is a Cisco IOS-based solution which integrates the Cisco VPN solutions with Cisco dynamic protocols framework.

- Failover/Load-balancing/SLB
- Dynamic routing
- Full – mesh and partial - mesh topologies.
- Hub-to-spoke and spoke-to-spoke tunnels.
- Permanent and on-demand tunnels

DMVPN is build on
- IPSec (RFC 2401)
- Next Hop Resolution Protocol (NHRP)
  Hub maintains a (NHRP) database of all the spoke’s routable (public interface) addresses
  Each spoke registers its routable address with the NHRP server (hub) after successful negotiation of the IPSec tunnel
  Spokes query NHRP database for routable addresses of destination spokes to build direct tunnels
- Multipoint GRE tunnel interface
  Allows GRE interface to support multiple IPSec tunnels
  Simplifies size and complexity of configuration
Standard DMVPN Design

DMVPN hubs

Corp. FWs

Spokes
DMVPN: Key Differentiators

- DMVPN uses crypto profiles and tunnel protection; this frees the physical interface from a crypto map.
- Management is performed over a separate VPN tunnel independent of the primary DMVPN data tunnels.
- DMVPN allows for dynamic registration of spokes:
  - One tunnel interface on the hub side supports a single DMVPN cloud
  -Eliminates static point-to-point configurations
  -Reduces the complexity of the hub configuration.
- DMVPN provides dynamic full and partial mesh capability:
  -Provides improved support for applications such as voice and video.
Server Load Balancing (SLB) Overall design

Corporate network

Aggregation router

Hubs
Cluster of DMVPN hubs
Aggregates user tunnels

Server Load Balancer
SLB balances connections
Owns virtual IP address

Spokes
GRE/IPsec tunnels
IGP + NHRP
DMVPN and SLB design

- Server Load Balancing (SLB) design of DMVPN is an enhancement of DMVPN and can be delivered in two different ways:
  - **Design one – DMVPN High concentration hub**
    Typically Cisco 7600 Series router or Cat65K acts like primary tunnel termination Hub and perform encryption and decryption functions.
    A farm of 7200 Series routers are associated with the IPSec termination device and handles all tasks related to Next-Hop Resolution Protocol (NHRP) and multipoint generic routing encapsulation (MGRE).
  - **Design two – DMVPN IOS SLB hub**
    The front device – typically Cisco 7200 or Cisco 7600 Series router performs the role of Load Balancer.
    A farm of 7200 Series routers are associated with the load balancer and handles all the tasks related to Next-Hop Resolution Protocol (NHRP) and multipoint generic routing encapsulation (mGRE) and IPSec encryption/decryption.

- Both design solutions have their advantages and disadvantages and based on the existing documentation and lessons learned, SLB design provides the following advanced enhancements for DMVPN:
SLB DMVPN – Key Advantages

- SLB is much easier to configure and support, since the configuration of the peer tunnel IP is always the same no matter how large is the deployment. The peer IPSec IP (the termination device’s tunnel IP) acts like a cluster IP and does not change due to design or scalability considerations.

- SLB scales higher, since the EIGRP – based scalability restrictions are mitigated and the number of tunnels is virtually limitless.

- SLB provides higher tunnel creation rate, recovers faster when cluster node becomes unavailable and provides spoke to spoke functionality as the standard DMVPN does.
SLB DMVPN – Key Advantages (Contd.)

- SLB provides better redundancy.
  
The standard DMPVN design provides redundancy in pairs – the dual tunnel, single layout design (from CPE) actually terminates the CPE to two separate SDGs, maintaining active-active status of the crypto tunnel connections. In that case, the number of the primary hubs is actually equal to the number of the backup hubs and the total number is 2N.

  Everything equal, in SLB if we assume the same number of CPEs per Hub (pair of hubs) the number of Hubs in SLB design should be N+2 (assuming dual SLB head end design).

- SLB design can provide fully redundant solution, where in dual SLB design the CPE can connect to a pair of farm hubs, which are not geographically co – located. In other words in its extreme the solution can allow CPE to fail over to another hub, located in another part of the same campus, or the SLB pair to fail over to another pair of hubs, located in another geographical location.
NG ECT Solution and Low TCO – End-to-End Provisioning with Cisco Security Manager
Cisco Security Manager

- CSM Manages Devices - PIX Firewall, ASA, FWSM and Cisco IOS routers
- It manages transport mechanisms, such as SSL, Telnet, HTTP, HTTPS, TMS and Cisco Networking Services (CNS) working with CE 2.0.
- CSM Manages Policies, activities and objects.
- It manages Site to Site VPNs, Remote Access VPNs, SSL VPNs and Easy VPNs.
- CSM Manages Firewalls. Firewall Services manages firewall-related policies in Security Manager that apply to the adaptive security appliance (ASA), PIX Firewall (PIX), Firewall Services Module (FWSM) installed in a Catalyst 6500/7600 device, and security routers running Cisco IOS (IOS).
Cisco Security Manager (Contd.)

- It manages Intrusion Prevention System (IPS).
- Supports open XML/SOAP interface and NB APIs enabling integration with existing enterprise management framework.
- Supports fully managed service functionality to notify the administrators for non-CSM initiated configuration changes.
- CSM manages provisioning, manages deployment and manages FlexConfigs.
Configuring CSM - The Sample Device and the Security Policies

- Create a sample device.

**New Device - Choose Method (Step 1 of ...)**

Please choose how you would like to add the device:

- **Add Device From Network**
  When you add a device that is live on the network, Cisco Security Manager makes a secure connection with the device and discovers its identifying information and properties.

- **Add from Configuration File**
  When you add a device using its configuration file, Cisco Security Manager discovers the device’s identifying information, properties and policies from the file.

- **Add New Device**
  You can add a device that is not yet on the network by specifying the device’s identifying information and credentials.

- **Add Device From DCR**
  If you are using other CiscoWorks applications and your devices have already been added to the device credentials repository, you can import them into Cisco Security Manager.
Configuring CSM - The sample device and the security policies

- Create a sample device.
- Configure the FW policies:
  - AAA Access Rules
  - Access Rules
  - Inspection Rules
  - Access Control
  - AuthProxy
  - Inspection
- Site to Site VPN – Large scale DMVPN - SLB config
- Quality Of Service
- Configure NAT – flex config based

- Start with single device
- Assign policies
- Define the policies as shared or local
Configuring CSM - The sample device and the flex configs

- Create a sample device.
- Attach 871 prepend config(s)
- Attach BASIC append config(s)
- Attach WIFI append config(s)
- Attach IPT append config(s)
- Attach VIDEO append config(s)
- Attach 871 append config(s)

• Start with single device
• Attach prepend and append flex configs, based on expected granularity
Cisco Security Manager 3.1
SLB Hub configuration

- Configure a Hub device
- Configure SLB device and interfaces.
- Create Hub and Spoke VPN
- Edit Hub and Spoke.
- Select devices for SLB
User Request for NG ECT Service
Eleven Steps to Provision and Deploy a Remote Router

- User submits the NG ECT request (changing/saving/etc) REQUESTED STATE
- Mgr approval triggers the processes APPROVED STATE
- EMAN Create ACS account on the ACS server as part of PKI&AAA config.
- EMAN Address Management: AM agent assigns /28 to every user.
- EMAN Host Management: Host record is created in EMAN for monitoring/tracking
Eleven Steps to Provision and Deploy a Remote Router (Cont…)

- EMAN Template Management – the device is associated with the predefined set of templates.
- EMAN Address Management: AM agent assigns /32 ip address for the tunnel interface.
- TFTP IP address supplied by EMAN out of TNM.
- CS-M cloning (6 sub-steps within the CS-M):
  - CNS configuration staged
  - SDM/SDP process - configuration downloaded to the CPE router & the state changes to OPERATIONAL
Cisco IT Implementation – CSM Integration using APIs.
Cisco Security Manager 3.1
6 Easy CPE Provisioning Steps

- Clone a device from SAMPLE-SJC-871-ONE
- Set device properties – Transport protocol
- Set device properties – Interface roles
- Set device properties – Set Networks/Hosts
- Set device properties – Set Text Objects
- Edit QoS policy
- Submit and Deploy
NG ECT Solution and Low TCO – End-to-End Deployment with Cisco Security Manager
Conventional Deployment of Spoke Routers

- In-house; router configured by IT
- Outsource to ISP; router configured at staging facility
- Outsource to 3rd party; router configured at staging facility or on-site

All Three Methods Add Excessive Cost to the Deployment Process!
NG ECT Offers Four Deployment Options

- **Zero Touch Deployment.**
  User responsible for configuring router for Internet access and running SDP (Secure Device Provisioning)
  Policy configurations are pushed over the CNS transport mechanism

- **On-line (Cert-Proxy)**
  Allows engineer to configure router remotely

- **E-Token Based Secure Device Provisioning**
  Allows engineer to configure router remotely

- **Off-line - Special cases/configurations and pilot environments**

- **Regardless of the deployment option, spoke router provisioning process is automated to minimize TCO**
ECT CPE ZTD Deployment

- Spoke router performs SDP and obtains keys and certificates.
- Management GW authenticates spoke router using PKI-AAA integration
- Spoke router establishes mgmt tunnel, “calls home” and sends CNS “connect” event to CE Engine.
- CE pushes & audits policy over management tunnel
- Spoke router establishes VPN tunnel w/Data GW1, gains access to corporate resources
- VPN tunnel established w/Data GW2 and stays active for failover.
Today the ECT solution uses ‘Auth Proxy’ to authorize PC’s to corporate resources.

- Auth Proxy uses a userid and Active Directory (AD) password through a browser.
- Once the user has successfully authenticated, corporate resources (email, IM, etc) can be accessed.
- If the authorization is not successful, the PC can still access the internet.
ROI, TCO and ZTD Cumulative Cost Savings

ZTD Assumptions:

- User's time (minutes) working w/ support to set up router: 45
- Engineer time (minutes) spent configuring router: 120
- Engineer time (minutes) confirming user set up: 10
- Percent of users requiring router set up support: 100%

Percent users requesting engineer follow-up after set up: 30%
Annual "Fully Loaded" Salary per Employee: $140,000

ECT Router Configuration Cost:
- Engineering support cost per router: $149.48
- User cost to set up router: $56.69
- Average cost for engineer to ship router to user: $35.00
- Total cost per router: $239.17

ECT Deployment Costs:

<table>
<thead>
<tr>
<th></th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual ECT User Adoption</td>
<td>7250</td>
<td>2750</td>
<td>4500</td>
</tr>
<tr>
<td>Manual Router Set Up Costs</td>
<td>$1,783,938</td>
<td>$777,252</td>
<td>$1,076,250</td>
</tr>
<tr>
<td>Operational ECT Costs</td>
<td>$10,981,458</td>
<td>$5,199,167</td>
<td>$7,070,000</td>
</tr>
<tr>
<td>Total Operational ECT Costs</td>
<td>$12,715,417</td>
<td>$5,976,458</td>
<td>$8,146,250</td>
</tr>
</tbody>
</table>

ZTD Cost Savings:

<table>
<thead>
<tr>
<th></th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZTD Engineering Headcount Reduction</td>
<td>9</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>ZTD Cost Savings</td>
<td>$1,738,593</td>
<td>$777,252</td>
<td>$1,076,250</td>
</tr>
<tr>
<td>ZTD Cost Savings Percentage</td>
<td>13.64%</td>
<td>13.01%</td>
<td>13.21%</td>
</tr>
</tbody>
</table>

ZTD Cumulative Cost Savings:

<table>
<thead>
<tr>
<th></th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZTD Cumulative Cost Savings Percentage</td>
<td>$3,587,500</td>
<td>13.37%</td>
<td></td>
</tr>
</tbody>
</table>

*Operational ECT Cost breakdown available in the ECT Return on Investment (ROI) Tool.
The Eser’s Experience

I wanted to let you know my first hand experience with my new ECT router and getting it set up. I dreaded the process. My last ECT router was shipped to me with a very large book on how to configure it. The new router sat in a box next to my desk for about 4 days because I was planning to dedicate a full weekend to the process of hooking it up and getting it configured.

Well, much to my surprise, I hooked everything up (including my home equipment) and had the new router configured in 15 minutes! Let me repeat that, 15 minutes. The instructions on the Web and the printed material was easy for a non-technical person to understand, the router was set up to be configured and connecting to the site for configuration was easy.

Wala! 15 minutes later I am back in business. It even amazes me that I was able to do it without hassle.

Now back to work!!!!! But from home!!!!!

Sincerely yours,

Pat Moore, Mgr, Workplace Resources
NG ECT Solution and Low TCO – End-to-End Management with Cisco Security Manager
TCO and Lower Costs of Management
TCO and Utilizing Reusable Components

- Integration of CSM and CNS-CE into EMAN
- Monitoring – EMAN based
- Analyzing / Grouping – static and dynamic groups.
- Automated Decision making
- Automated Deployment options: EMAN/CSM/CE based.
  - Event - triggered deployments
  - Scheduled deployments
  - Rapid deployments - push/pull policies and ACLs.
  - Regular deployments – once per 24 hours.
    Example - over night password management.
  - IOS management is based on EMAN/CNS-CE functionality
TCO and Automation of routine operations
MAJOR AUTOMATION WINS

- Migration from one device/platform to another.
- Connection Type change
- Upload speed change – UP or DOWN.
- Service MOVE from one location to another.
ISC to CS-M Migration. Platform A to Platform B Migration
ZTD of IPT for Remote Access

- User applies for the IPT service as part of their ECT service and upon approval orders their IP Phone or installs IP Communicator (IPC); an additional instance of a phone is configured for the employees Dialed Number (DN) on the Cisco Call Manager (CM)
- IPT device is shipped from factory.
- ECT router is successfully configured and has established data tunnels; user connects the IPT device to the ECT router
- When the IPT connects to the fully functional ECT router, the universal loader will be loaded to the IPT and the IPT will boot and obtain an IP.
ZTD of IPT for Remote Access (Contd.)

- The CCM will register the MAC address of the IPT and it will assign a random DN to the phone, which will appear on the IPT’s screen.
- The user will use URL application to connect to a server. The user will be authenticated and prompted for user credentials.
- Upon successful authentication the user will enter the random DN, shown on the screen on the IPT.
- The backend script will replace the random DN with the previously assigned DN to the user. The IPT will obtain the associated profile from TFTP server and it will connect and register with the CCM.
Service Oriented Architecture over VPN. QOS, IP SLA and Lessons Learned
QOS and Minimum SLA Requirements

• Applications with similar QoS requirements are grouped into a service (traffic) class (e.g., Voice, Interactive Video as real-time)
• Service Classes will have separate loss, latency, jitter requirements:
  - Time Sensitive class—Voice, Interactive Video
  - Business critical class—Oracle, SAP, WebEx, MeetingPlace
  - Best effort - Internet access, file transfer
  - Scavenger class – TLM and Streaming video

• Every map class later is associated with a separate policy.

<table>
<thead>
<tr>
<th></th>
<th>PoP-to-PoP</th>
<th>End-to-End</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Real Time</td>
<td>Business</td>
</tr>
<tr>
<td>Loss</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Delay</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Jitter</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Availability</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
| Contracted BW  |            |            | ✔  | ✔         | ✔        | ✔  | (cBW)
## IP SLA Metrics

<table>
<thead>
<tr>
<th>Minimum SLA Attributes Related to QoS</th>
<th>Other SLA Attributes related to QoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latency (Delay)</td>
<td>Availability</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Mean Time to Repair (MTTR)</td>
</tr>
<tr>
<td>Delay Variation (Jitter)</td>
<td>Mean Time Between Failure (MTBF)</td>
</tr>
<tr>
<td>Contracted Bandwidth</td>
<td>Per-Flow Packet Sequence Preservation</td>
</tr>
<tr>
<td>Throughput</td>
<td>Admission Control Criteria</td>
</tr>
<tr>
<td>Contention Ratio</td>
<td>ISP supported QoS at the edge</td>
</tr>
</tbody>
</table>

SLA measurement/reporting tools - measurement points, methodology, reporting methodology (web, e-mail) reporting interval, report contents, failure criteria and penalty clauses.
IP SLA Requirements for IPT@Home and Interactive Video@Home

- Loss should be no more than one percent.
- One-way latency should be no more than 150 ms.
- Jitter should be no more than 30 ms.
- Voice (bearer) traffic should be classified as EF, or with TOS=5.
- Call signaling traffic should be marked as AF31/CS3.
- The codec type should not be a factor when configuring IPT for Home. The reason is that jitter and out-of-order packets cause more audio signal damage with G.729 than G.711.
- Interactive video traffic should be classified as AF41 or marked with TOS=4/TOS=2.
- The minimum priority bandwidth guarantee (LLQ) or CBWFQ is the size of the video conferencing session plus 20 percent. (For example, a single 384 kbps video conferencing session requires 460 kbps of guaranteed priority bandwidth.)
Other QoS and IP SLA Requirements

- **Streaming video** (whether unicast or multicast) should be marked to CS3.
  Loss should be no more than 2 percent, latency should be no more than 4–5 seconds (depending on video application’s buffering capabilities). There are no significant jitter requirements.

- **Locally-Defined Mission-Critical class.** Transactional and interactive applications with a high business priority:
  - Transactional/Interactive - Client-server applications, messaging applications. The Transactional/Interactive class is a combination of two similar types of applications: transactional client-server applications and interactive-messaging applications.
  - Bulk/Non-Interactive - Large file-transfers, e-mail, network backups, database syncs and replication, video content distribution. Bulk applications can dynamically take advantage of unused bandwidth and thus speed up their operations during non-peak periods.

- **Best-Effort** – It is recommended that at least 25 percent of a WAN link’s bandwidth be reserved for the default Best Effort class.

- **Scavenger class.** “less-than Best-Effort” services to certain applications.

- **Routing and Network Management class.** It is an optional class of service and includes minimal bandwidth queue for routing and other network control applications, such as SNMP, NTP, Syslog, and NFS, EIGRP, and ISAKMP.
IP SLA Statistics - Example

rcdn-user-871#show ip sla status

Round Trip Time (RTT) for Index 10

  Latest RTT: 13 milliseconds
  Latest operation start time: 19:27:34.837 PDT Sun Oct 7 2007
  Latest operation return code: OK

RTT Values:

  Number Of RTT: 1000  RTT Min/Avg/Max: 10/13/26 milliseconds

Latency one-way time:

  Number of Latency one-way Samples: 1000
  Source to Destination Latency one way Min/Avg/Max: 1/2/14 milliseconds
  Destination to Source Latency one way Min/Avg/Max: 9/11/17 milliseconds

- Jitter:

  Number of Jitter Samples: 999
  Source to Destination Jitter Min/Avg/Max: 1/1/13 milliseconds
  Destination to Source Jitter Min/Avg/Max: 1/1/6 milliseconds

- Packet Loss Values:

  Loss Source to Destination: 0  Loss Destination to Source: 0
  Out Of Sequence: 0  Tail Drop: 0  Packet Late Arrival: 0

- Voice Score Values:

  Calculated Planning Impairment Factor (ICPIF): 1
  Mean Opinion Score (MOS): 4.34
Lessons Learned

- Select hub locations to optimize latency and keep it under certain threshold.

- Start with limited pilot
  - Become familiar with technology, grow to 100.
  - Understand information requirements and system flow and scale.
  - Deploying the technology to multiple segments of the network allows IT organizations to maintain low TCO.

- Plan phased approach for new services. SLAs and IP SLAs for the services is must.

- Use CSM – CE to deploy and manage the environment. For large scale deployments use NB APIs to integrate these management platforms into the existing management environment.

- Automate all the routine operations.

- Develop a proactive monitoring and support. Allow the support engineers to participate in the pilot phase.
More Networked Home/Access Resources

Case Studies
http://www.cisco.com/web/about/ciscoitatwork/case_studies.html

Call to get Product, Solution and Financing Information
1-800-745-8308 ext 4699

Other Resources
