Collaboration Techtorial

Čas	Přednáška	Přednášející
10:45 - 11:30	Bezpečné připojení mobilních klientů	Jaroslav Martan
11:45 - 12:30	Návrh číslovacího plánu, URI dialing	Ivan Sýkora
13:30 - 14:15	Videokonference pro pokročilé	Jan Račanský
14:30 - 15:15	Pohled do nitra virtuálních desktopů	Tomáš Horák
15:30 - 16:15	API - Jabber SDK, Cius	Jaroslav Martan

Phone VPN
&
Secure Connect

Jaroslav Martan, CSE, CCIE #5871
e-mail/im:jmartan@cisco.com, video:jmartan@jabber.com

Prosíme, ptejte se nás

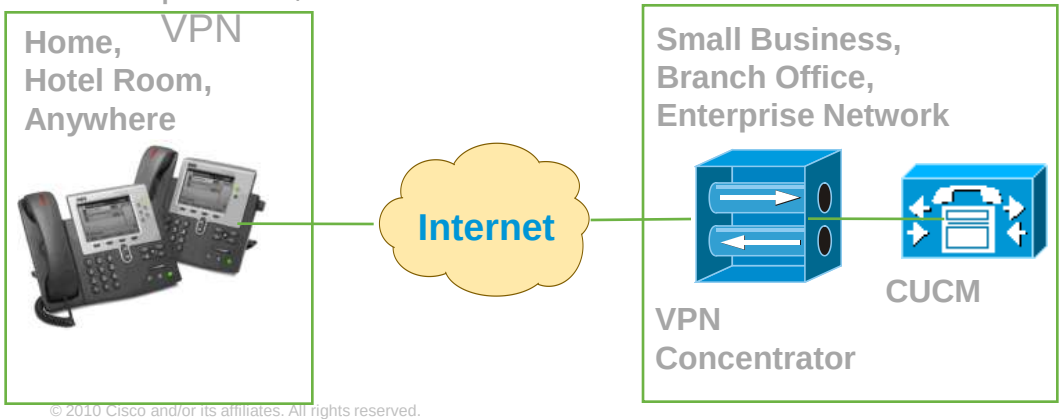
- Twitter www.twitter.com/CiscoCZ
- Talk2cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600

Agenda

- Feature Overview – benefits, devices
- CUCM Configuration
- Working with the phone

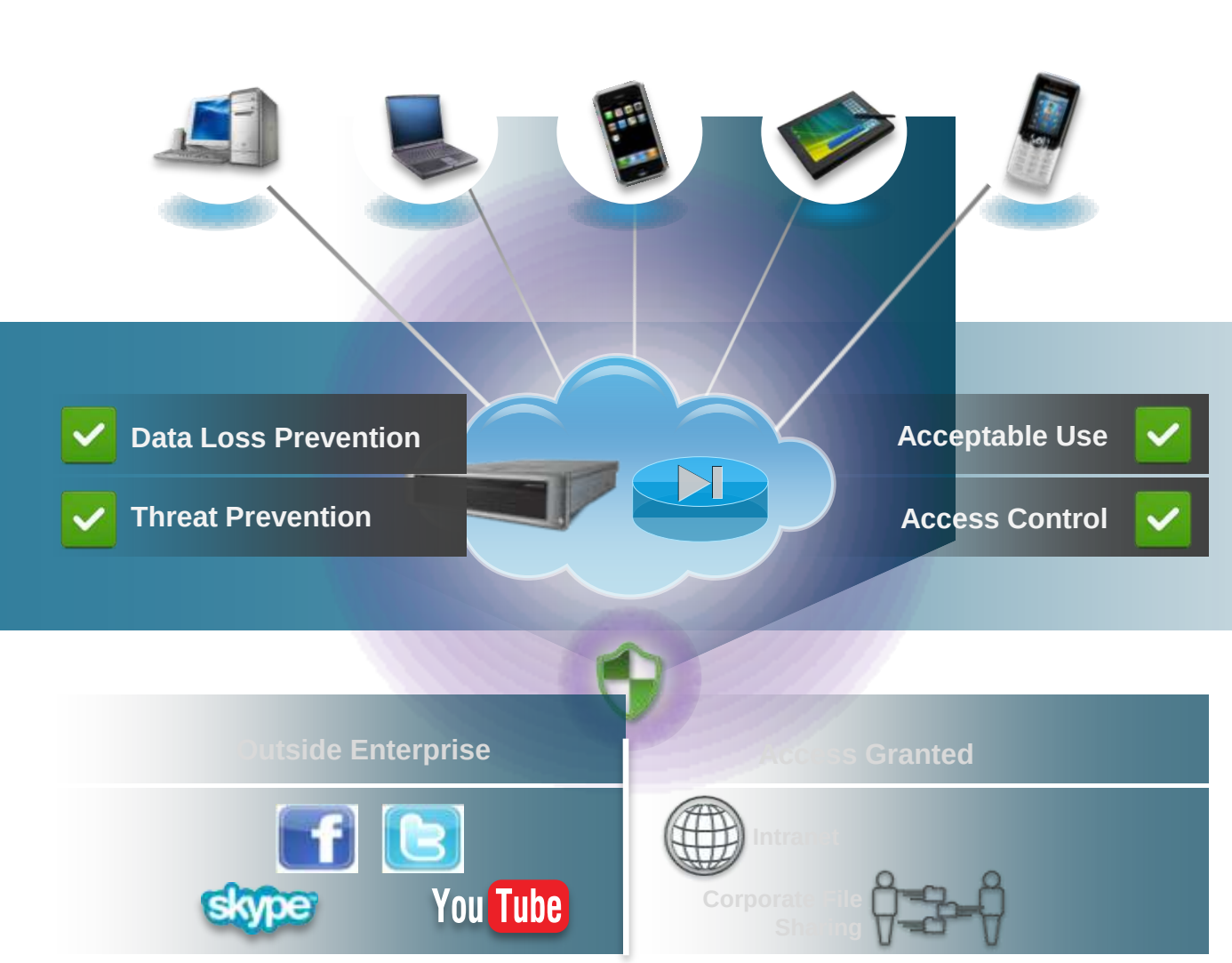
VPN Client for IP Phones

- **Easy to Deploy** – All settings configured via CUCM administration
- **Easy to Use** – After configuring the phone within the Enterprise, user takes it home and plugs in into their broadband router for instant connectivity. No difficult menus to traverse.
- **Easy to Manage** – Phone can receive firmware updates and configuration changes remotely
- **Secure** – VPN tunnel only applies to voice and IP phone services. PC connected to PC port responsible for authenticating and establishing own tunnel with VPN client software
- **VXI Integration** – the VPN can be used by the Cisco integrated VXI client for 99xx and 8961 phones, other devices have to create their own VPN



Cisco VPN Client	
Endpoint support	▪ SCCP: 7942,7945,7962,7965,7975 ▪ SIP: 8961, 9951, 9971 ▪ IPv4 Only
Deployment mode	▪ IP Phone Remote Access
Services secured	▪ Voice ▪ Data (Phone Services)
Licenses	▪ VPN Premium License ▪ No special license on CUCM
VPN Concentrators	▪ Cisco ASA 5500 Series ▪ Cisco ISR with IOS SSL VPN
Encryption Technology	▪ Secure Socket Layer (SSL)
Deployment Considerations	▪ No additional hardware needed at remote location other than IP Phone ▪ Concurrently running IP Phone Services Reduced When Enabled (i.e. no midlets)

Benefits of secure connect
Common Cisco Remote Access Infrastructure



Choice

Diverse Endpoint Support

AnyConnect Mobile Client or Cisco Jabber

Security

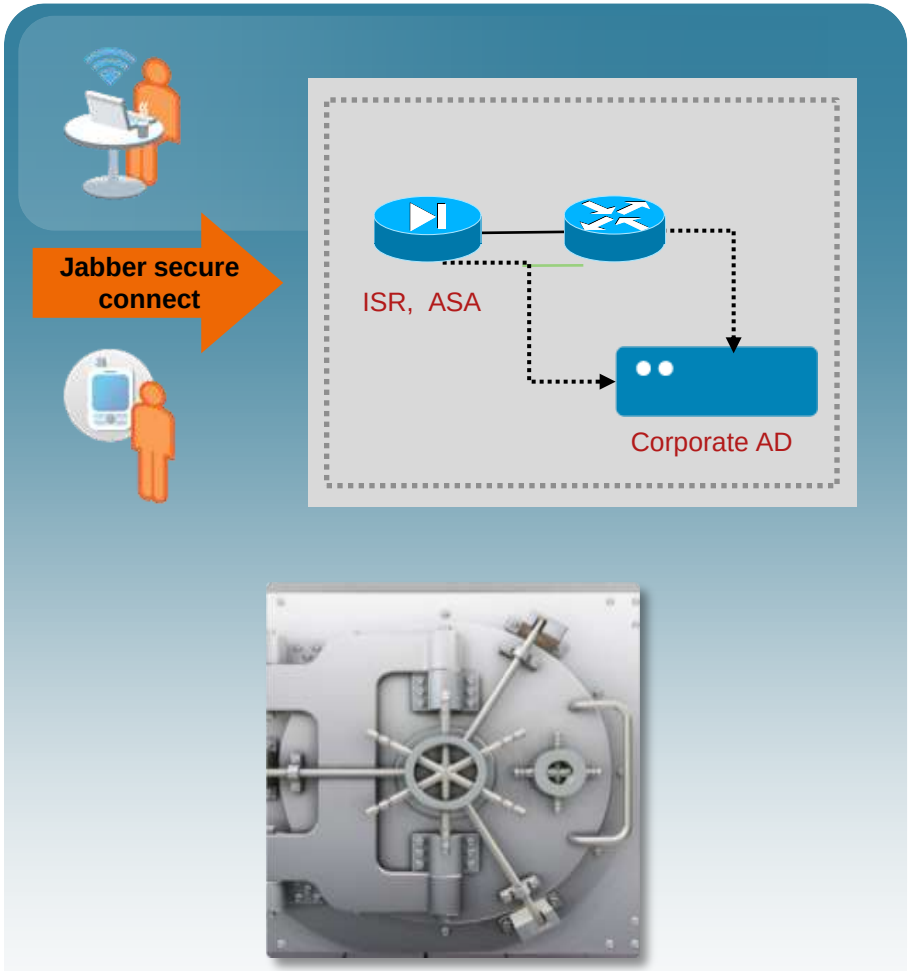
Security Integrated into the network

Experience

Always-on Intelligent Connection

Benefits of Secure Connect
Administrative Simplicity

- Jabber app integrates secure connect
- Backend scales with multiple Jabber applications
- Coexists with Cisco AnyConnect
- Utilizes highly secure, scalable and redundant Cisco infrastructure
- Common licensing, security design, policy and user management for AnyConnect & Jabber secure connect



Secure connect in Jabber & AnyConnect Differences and Similarities

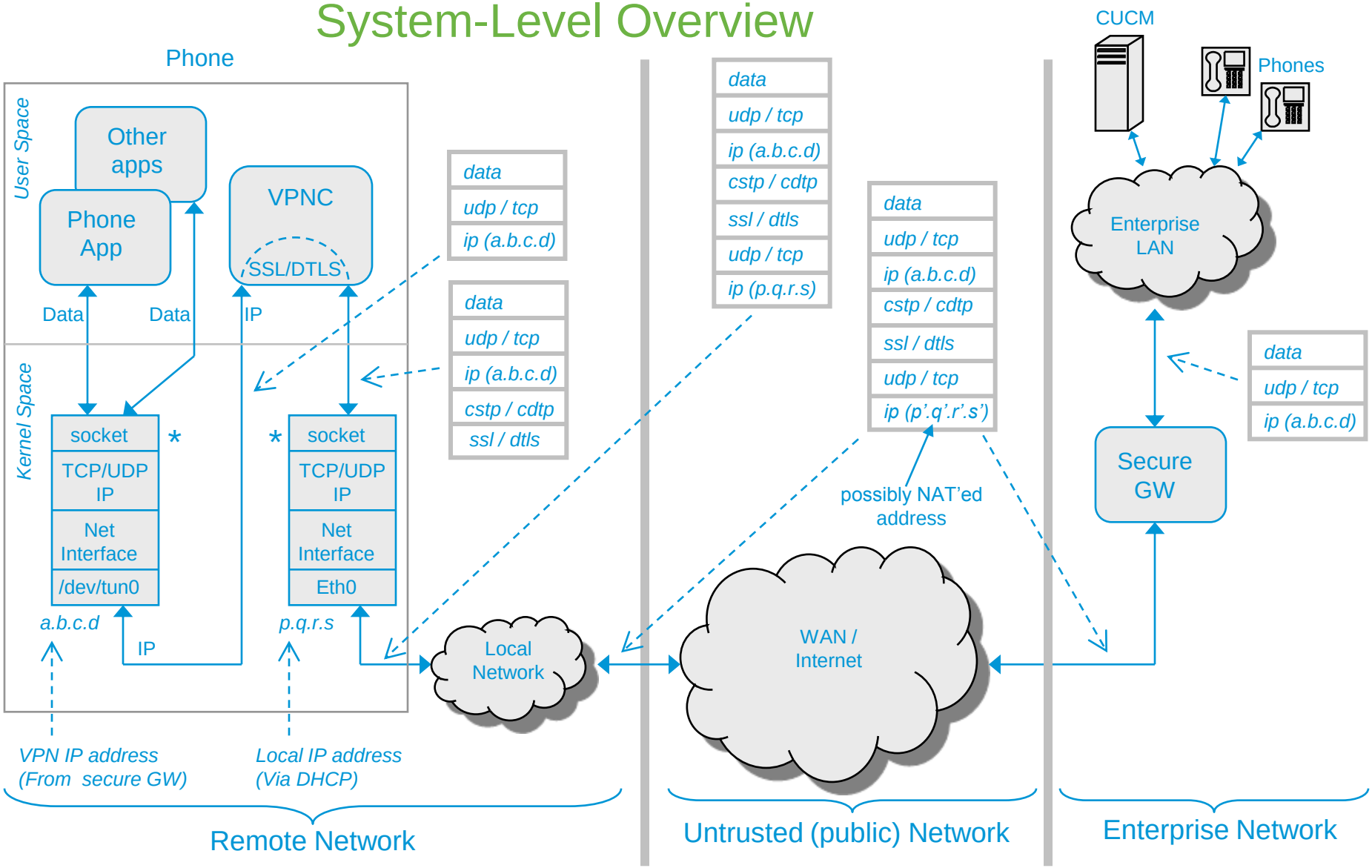
What does Jabber secure connect have that AnyConnect does not?

- Integration with Jabber for simplified user experience (pre + post install)
- Only Jabber traffic accesses enterprise network, not entire device
- Native access to local network resources
- Jabber has direct control of connectivity
- Jabber secure connect feature is not available yet for all Jabber apps; phased intro during 2011-2012

How are the Jabber secure connect feature and AnyConnect similar?

- Authentication, encryption, advanced security, protocol support (e.g. DTLS), shared code base
- Common infrastructure, provisioning, management, licensing
- Upgraded end-user experience over older, competitive VPN solutions
- Common security services available
- Both fully supported options with an ASA and ISR

SSL VPN Tunnel Operation
System-Level Overview

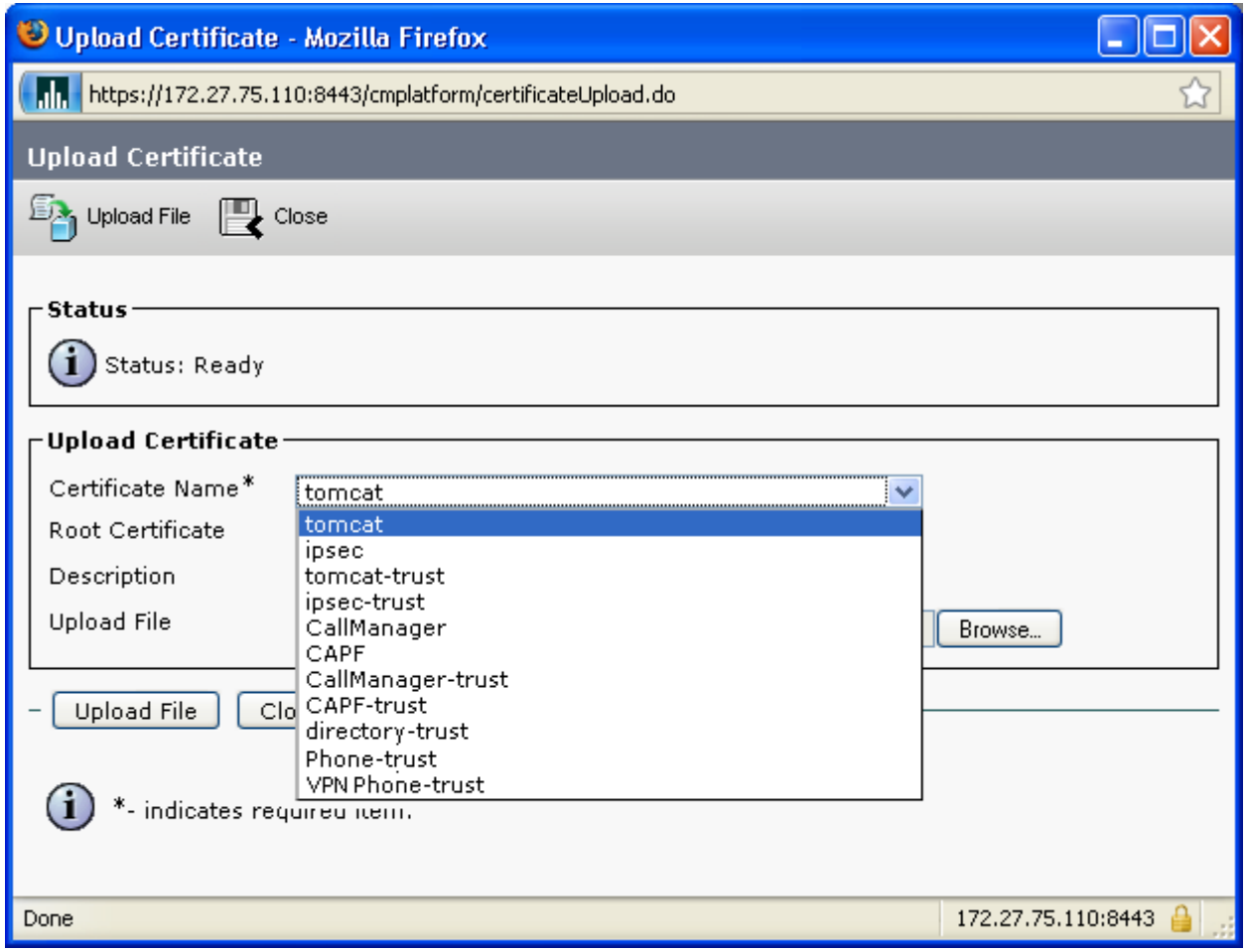


* *NOTE: The IP stacks are shown separately only for clarity, they are actually one and the same.*

UCM Administration
Configuring the VPN Feature on Supported IP Phones

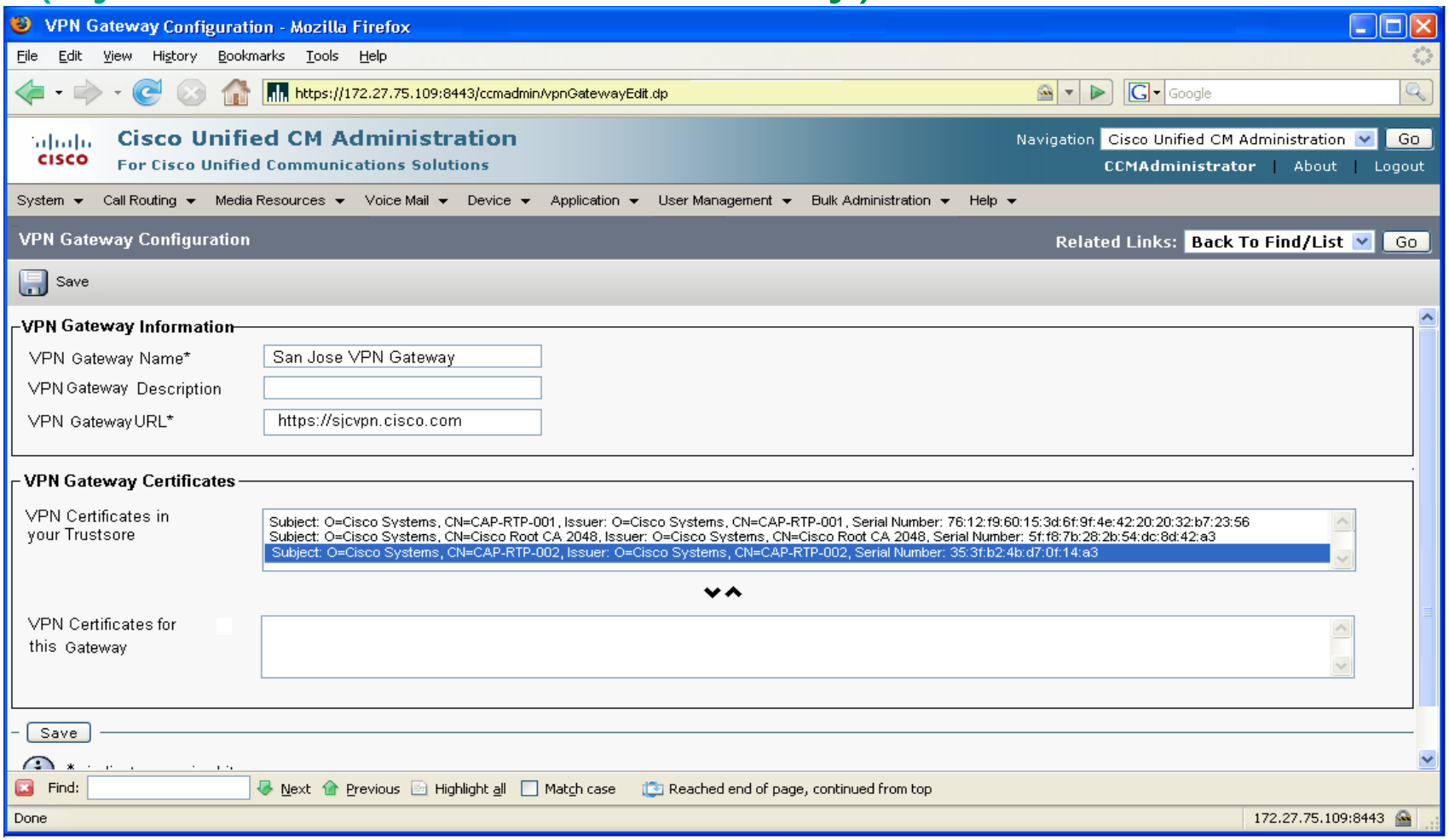
- Setup the VPN Concentrators for each VPN Gateway (not part of the UCM Administration and beyond the scope of this presentation)
- Upload the VPN Concentrator Certificates
- Configure the VPN Gateways
- Create a VPN Group using the VPN Gateways
- Create a VPN Profile
- Assign a VPN Group and Profile in the Phone Common Profile
- Phone is ready to be upgraded to a VPN supported phone load with this VPN configuration and certificate trustlist.

Upload the VPN Concentrator Certificates



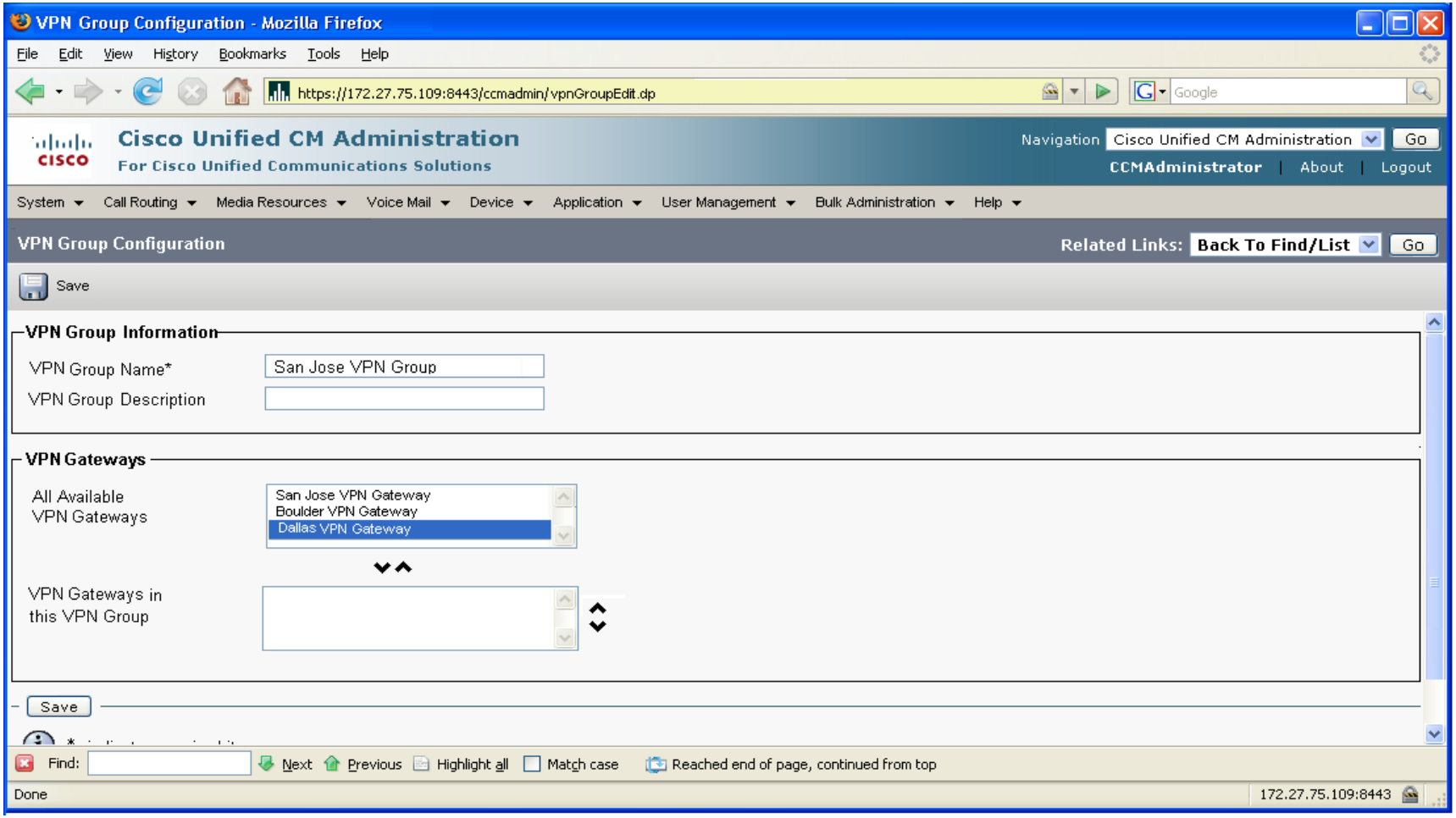
Use the Certificate Management GUI on the OS Administration page to upload the VPN certificates to a new VPN Phone-trust in the existing phone-trust store.

Configure the VPN Gateways (System->VPN->VPN Gateway)



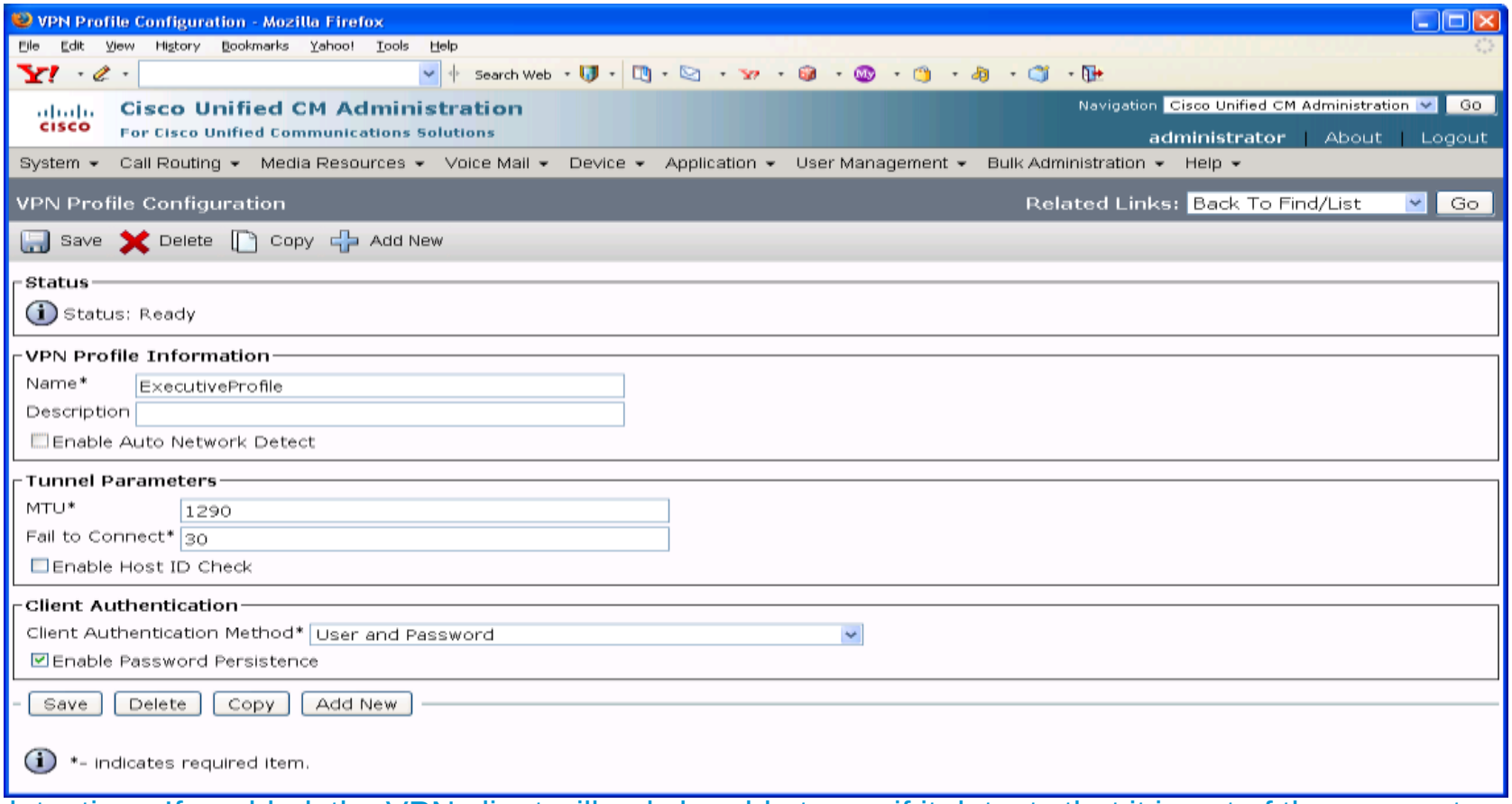
Up to 10 certificates can be assigned to a VPN Gateway. At least one must be assigned to each gateway. Only certificates associated with the VPN role shall show in the available VPN Certificates list. The URL should be for the main concentrator in the gateway.

Create a VPN Group using the VPN Gateways System->VPN->VPN Group



Up to 3 VPN Gateways can be added to a VPN Group.
The total number of certificates in the VPN Group can not exceed 10.

Create a VPN Profile
System->VPN->VPN Profile

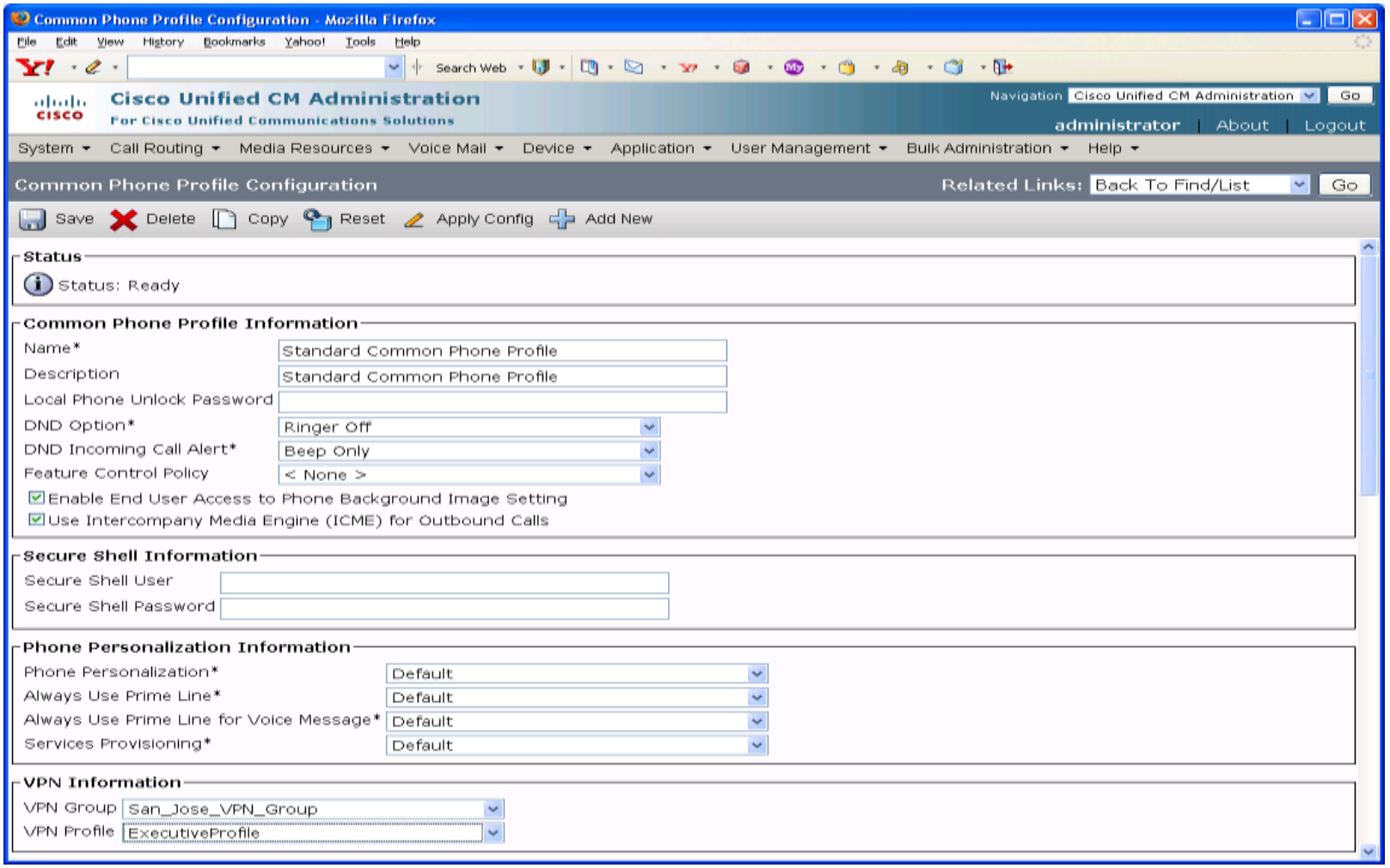


Auto detection - If enabled, the VPN client will only be able to run if it detects that it is out of the corporate network.

Enable Host ID Check - If enabled, the VPN gateway's certificate's subjectAltName or CN must match the URL that the VPN Client has connected to.

Enable Password Persistence - If enabled, a user's password will be saved in the phone until a failed login or a user clears it.

Assign a VPN Group and Profile in the Phone Common Profile Device->Device Settings->Common Phone Profile



A phone shall be in a specific VPN Group and assigned a VPN configuration Profile by associating with the corresponding Phone Common Profile.

IP Phone VPN Configuration and Status

- Inside the Enterprise
  - Upgrade to VPN supported phone load. (Must upgrade from load 8.4(4)+)
  - Pre-provision phone with VPN configuration and certificate trustlists
- VPN Setting in VPN Configuration Menu (Required to be set to establish a VPN Tunnel)
- Auto-Detect works in conjunction with the VPN Setting
- 'init.tab' modified to start the main process ('vpnu') associated with the VPN Client ('vpnu' subsequently starts child 'vpnc' process
- Feedback on the phone UI indicates VPN tunnel is being established, has failed to connect or is connected to one of the provisioned VPN concentrators.
- IPv4 Network Configuration on the phone UI shows network information (IP address, subnet mask, and DNS values returned from the VPN concentrator while establishing the VPN tunnel.

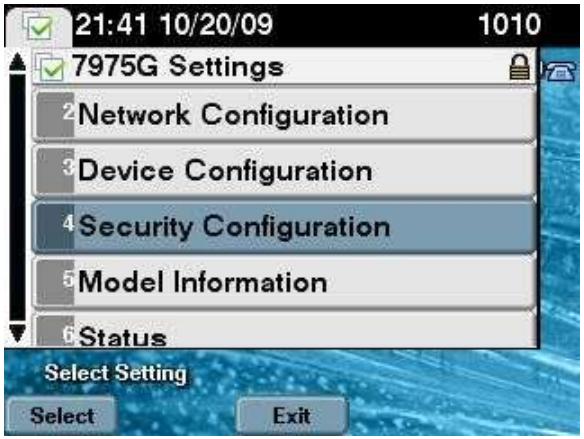
Establishing the VPN Connection

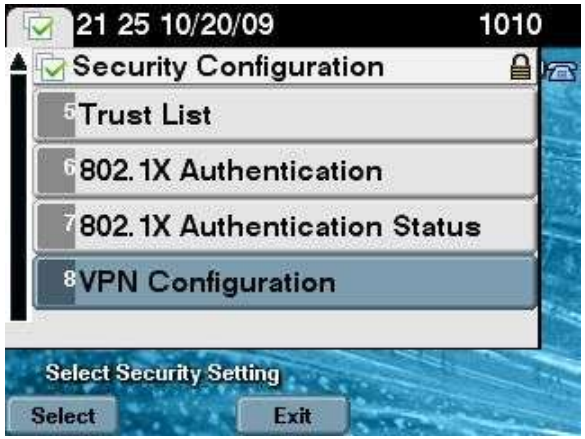
- The User can select whether the VPN Client (mode) is enabled or disabled in a phone menu.
- If the User *disables the VPN client*, the phone makes no attempt to create a VPN connection and proceeds with the standard startup sequence.
- If the User *enables the VPN client* and *auto-network detection is enabled*, the phone tries to detect the type of network, and attempts to create a VPN connection if appropriate.
- If the User *enables the VPN client* and *auto-network detection is not enabled*, the phone attempts to create a VPN connection. (Note: This opens up the possibility that a VPN connection can be established *within* the secure enterprise network)

VPN Client on the IP Phone

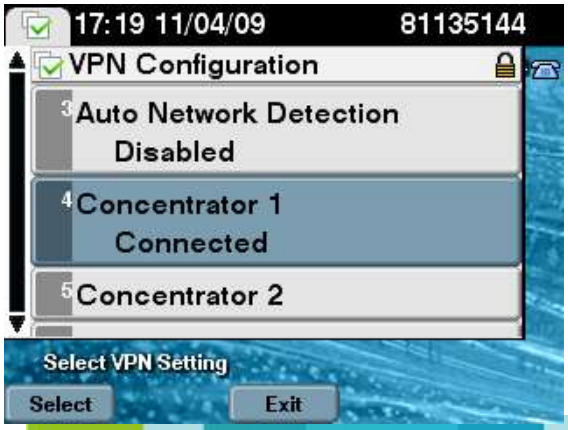
- Inside the Enterprise
  - Upgrade to VPN supported phone load.
  - Pre-provision phone with VPN configuration and certificate trust lists
  - ‘Alternate TFTP’ setting is configured to UCM or TFTP server IP address
- Auto-Network Detect works in conjunction with the VPN setting
- Feedback on the phone UI indicates VPN tunnel is being established, has failed to connect or is connected to one of the provisioned VPN concentrators
- IPv4 setup on the phone UI shows network information (IP address, subnet mask, and DNS values returned from the VPN concentrator while establishing the VPN tunnel
- VPN support over wireless (CP-9971)

VPN Client on the IP Phone



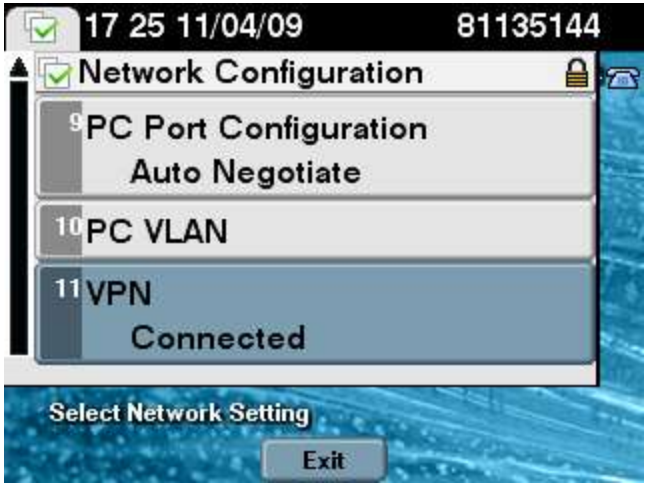


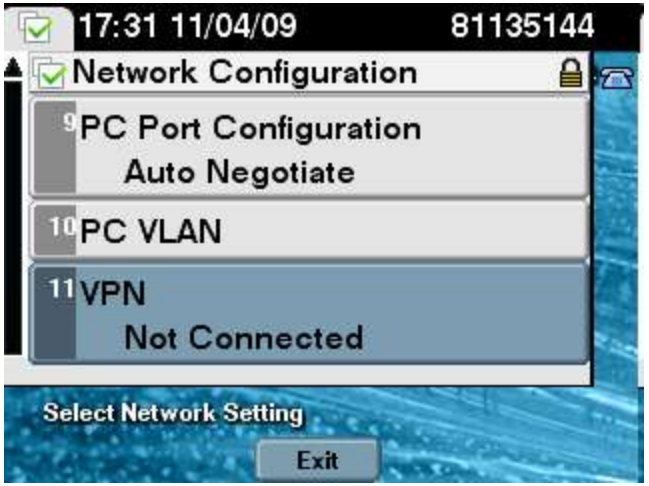
Settings ▸ Security Configuration ▸VPN Configuration



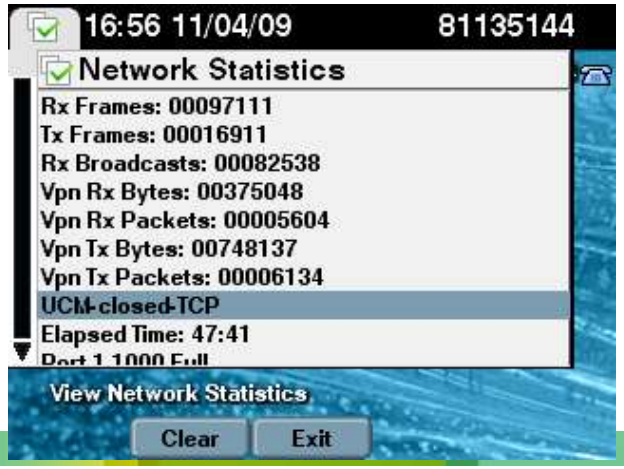
VPN Client on the IP Phone

Settings ▸ Network Configuration





Settings ▸ Status ▸ Network Statistics



Initial Authentication

- Phone contains new ‘VPN’ Application
- Three authentication methods (determined by admin)
  - User ID and Password
  - Certificate Only
  - Certificate and Password

Figure Sign In Screen for User ID & Password Authentication Mode

Phone Attempts VPN Connection…

- Status changes to show a connection attempt is in progress
- Toast message indicates successful connection
- VPN connection attempt can be cancelled In-process
- Alert to unsuccessful attempts, manual user re-try presented
- Auto-reconnect attempts can occur (same alerts and toast messages)

Figure Phone shows the toast indicating VPN connection is successful

Managing VPN Connections

- VPN can be Enabled ‘On/Off’
- User ID and Password can be changed or cleared

Figure User presses softkey to change credentials

Menu Changes to Support VPN Feature

- **VPN Login**

  Applications – New Menu created for VPN

- **Ethernet Data**

  Administrator Settings>Network Setup>Ethernet Setup

  Data in fields are overwritten when VPN connection is established

- **Status Messages**

  Administrator Settings>Status>Status Messages

  Additional Status Messages related to VPN feature operation

- **VPN Statistics**

  Administrator Settings>Status>VPN Statistics

  Current Connection: Rx/Tx data over VPN tunnel
  Past Connections: Last 10. Duration of connection. Reason for Disconnect.
  Failed Connections: Last 10. Duration of connection. Failure reason.

Summary

- Phone VPN
- Secure Connect
- Easy to use. Easy to administer

- Quiz:
  - Can I use my IP phone as VPN router?
  - Are there any exceptions?
  - How is RTP traffic transported? Is it TLS (TCP)?

Otázky a odpovědi

- Twitter www.twitter.com/CiscoCZ
- Talk2Cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600

- Zveme Vás na **Ptali jste se…** v sále **LEO**
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00

Prosíme, ohodnoťte tuto přednášku.