May 30, 2012

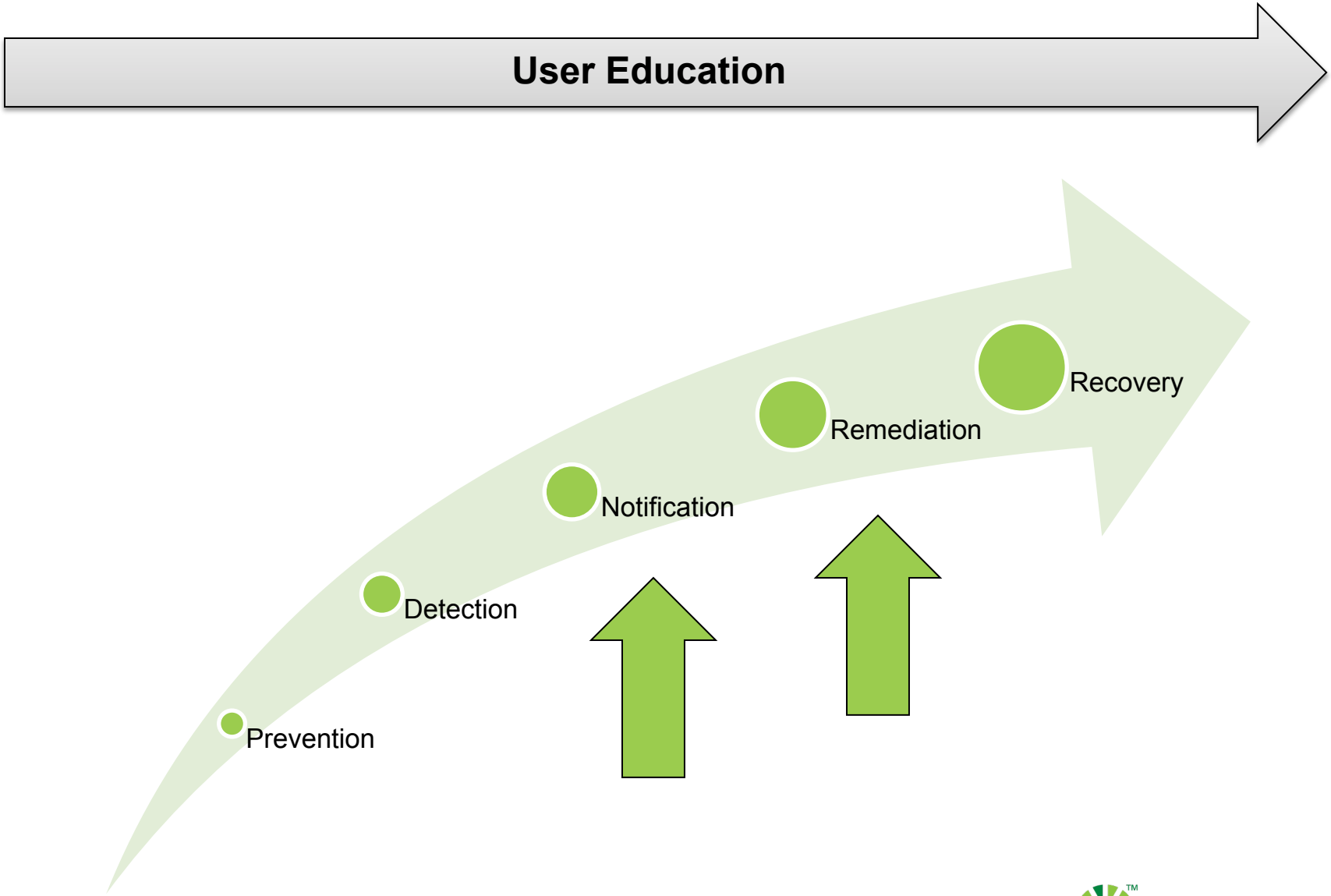
Malware Notification and Remediation Tools and Techniques

NIST Workshop: Technical Aspects of Botnet

Michael Glenn

CenturyLink™

5 Steps to Malware Remediation



CenturyLink™

Notification and Remediation Techniques

Method	Cost	Notify Effect	Remediate Effect	Pros	Cons
Email	Low	Low – Moderate	Low - Moderate	Cost	Easy to spoof Account DB
Telephone Call	Low - High	Moderate	Very Low - High	Cost	Account DB Cost
Postal Mail	High	Moderate	Low		Very Costly Remediation
SMS	Low	Low - Moderate	Very Low	Cost	Account DB
Instant Message	Low	Low - Moderate	Low	Cost	Easy to spoof Account DB
Walled Garden	Low	Medium - High	Medium - High	Direct Interaction	Infected Device Identification
Web Browser	Low	Medium - High	Low - High	Direct Interaction	Easy to Bypass

CenturyLink Notification & Remediation Program

Prevention

- Anti-virus Provided, Broadband Modem Firewall, NAT
- User Education Materials

Detection

- Rely on Trusted Third Party Reports
- Do Not Monitor Customer Traffic

Notification

- Leaky Walled Garden, Port 80 Web Traffic Redirection

Remediation

- 5 Step Process with Locally Hosted Tools
- Special Notifications and Tools by Malware Family

Consumer Internet Protection Program

Goals:

- Automate the notification of customers of AUP violations (today malware infected customers)
- Assist customers in a self help manner to clean their computers of the infection
- Educate users about the dangers of malware and good Internet security practices

System primarily **justified** through the lowering of tier 1 support calls. Additional benefits include:

- Better customer satisfaction with broadband product
- Lower customer churn
- Lower SPAM complaints
- Reduced level of DDoS attacks

Trial in January 2006, production release August 2006.

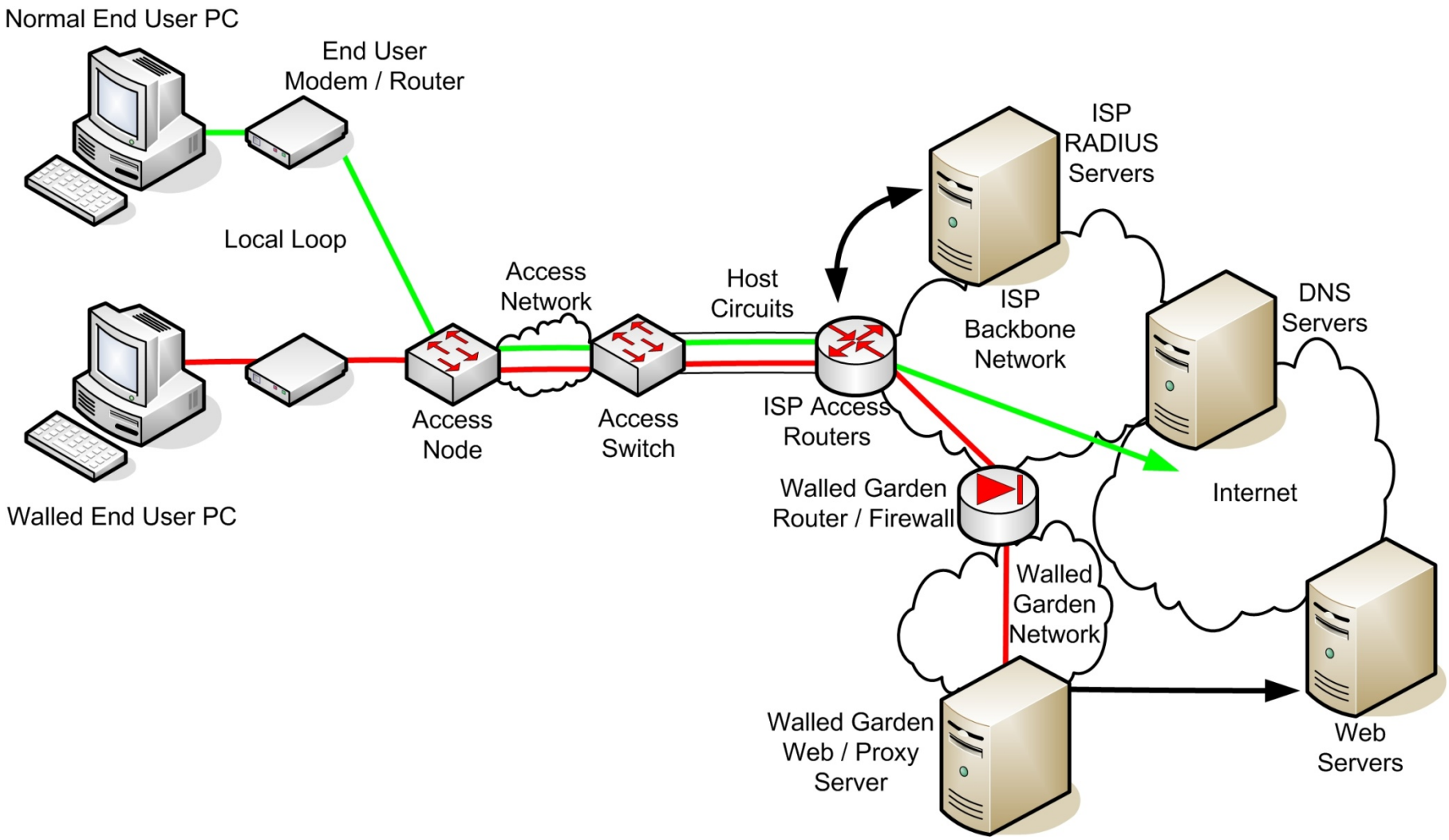
CenturyLink™

General Philosophy

- Assume majority of infected customers are not malicious, merely infected co-victims
- Treat them with respect
- Warn them of the risk to their personal information
- Educate them regarding good security practices
- Provide them self-help tools
- Do not lock them into the walled garden

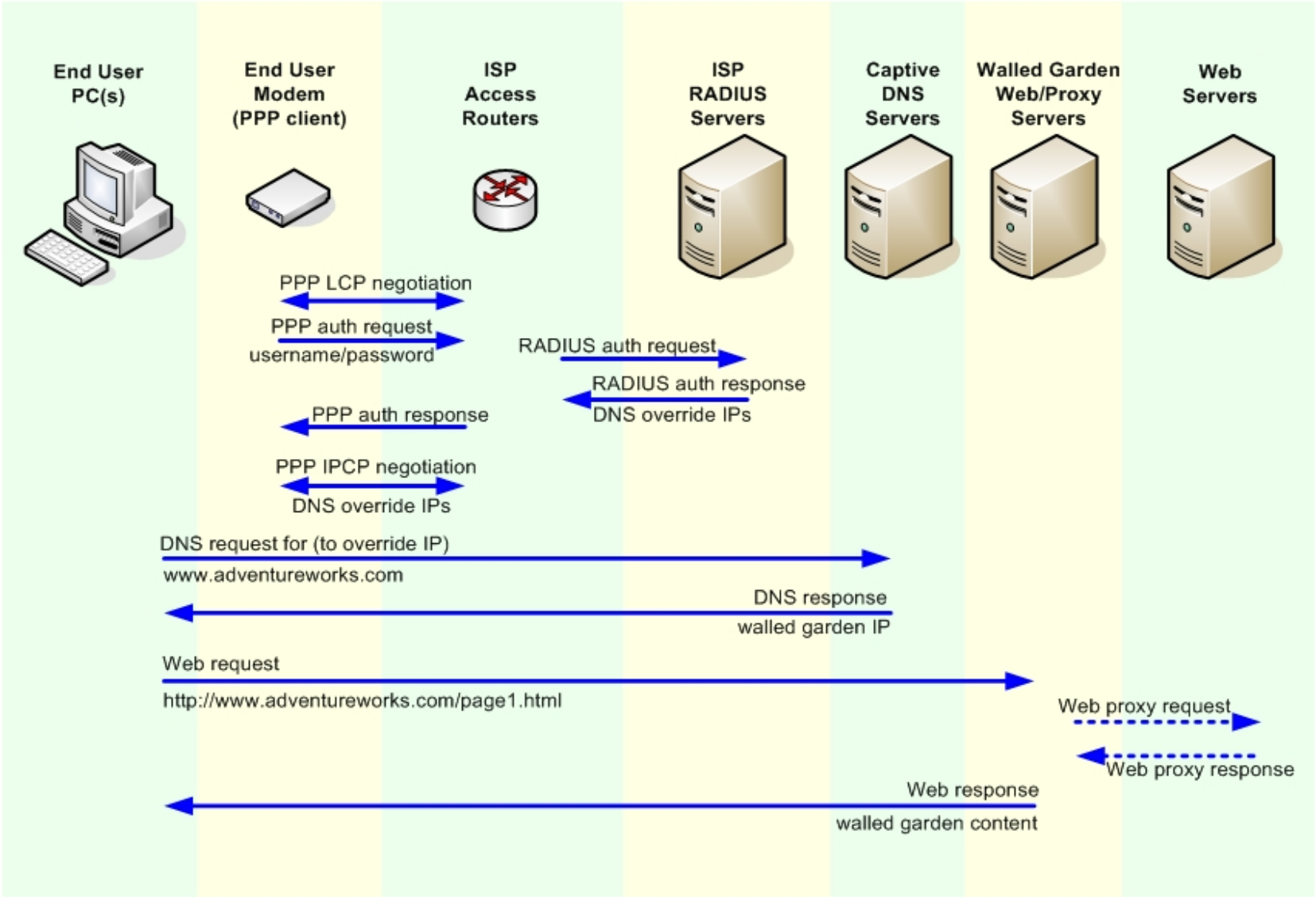
CenturyLink™

CenturyLink Botnet Notification & Remediation



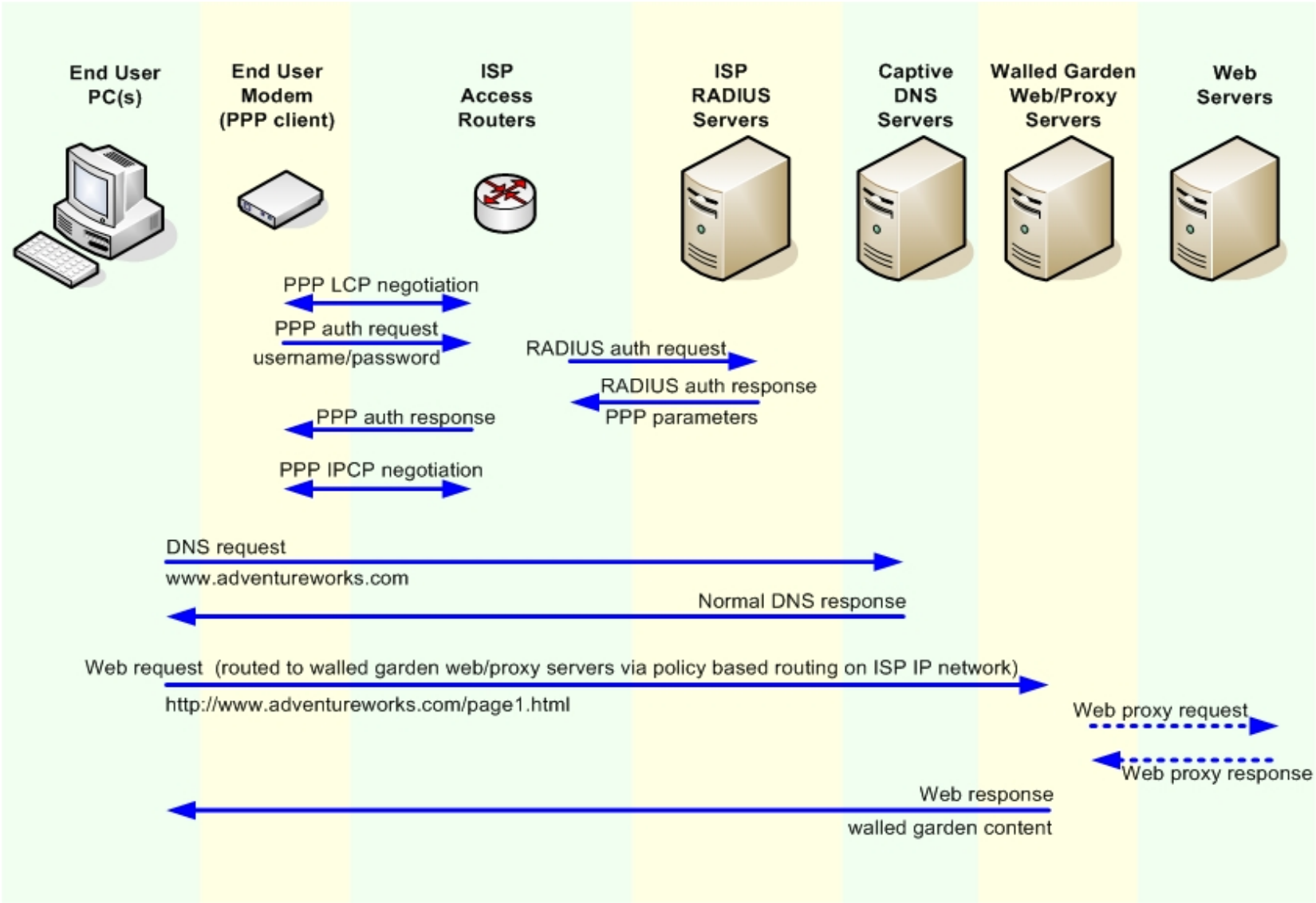
CenturyLink™

DNS Override



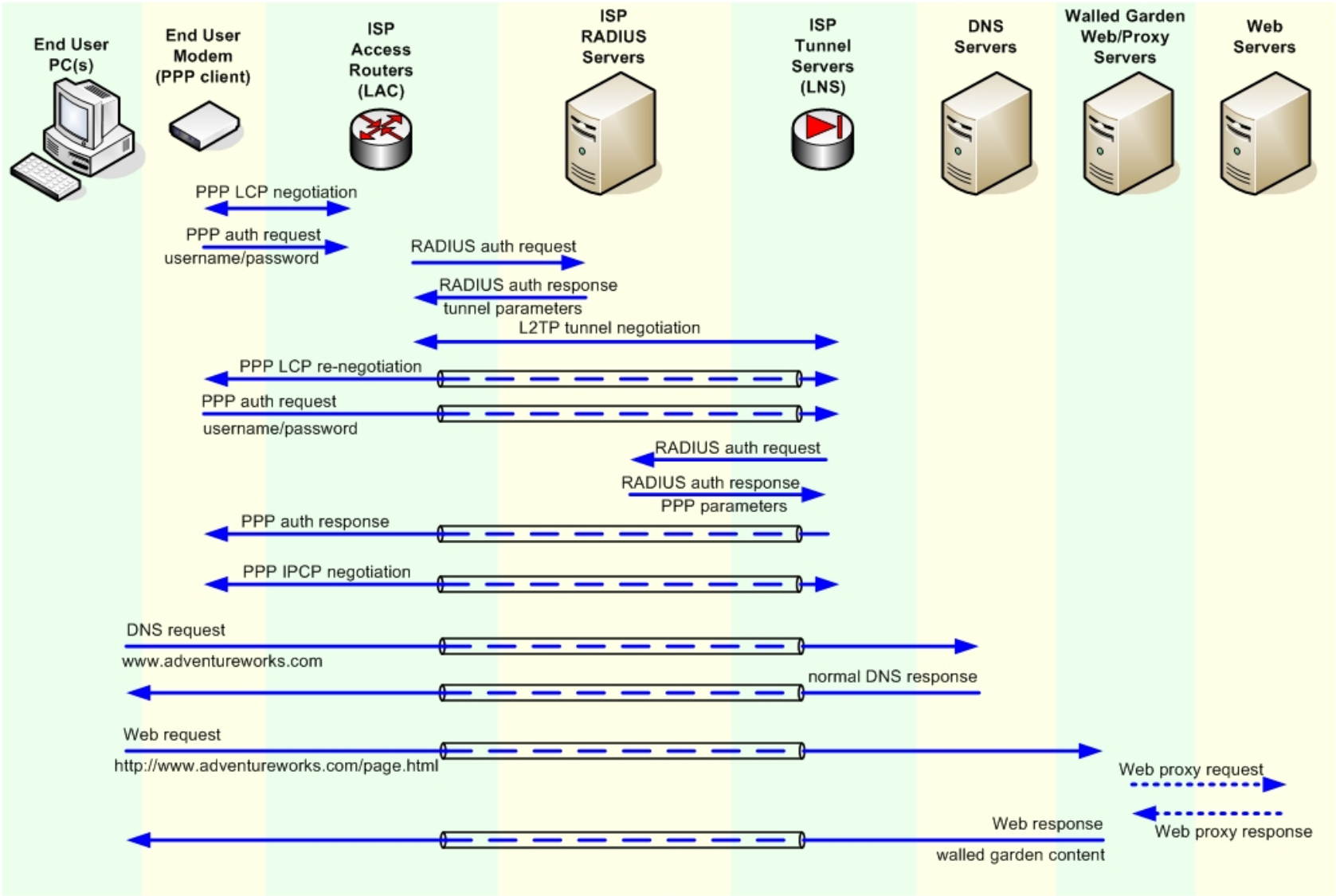
CenturyLink™

Policy Based Routing



CenturyLink™

Tunneled Traffic



CenturyLink™

Michael Glenn – Director Enterprise Security Technology
Email: Michael.Glenn at CenturyLink.com

CenturyLink™