



Metro Area EtherLECs and Security

David M. Piscitello

Core Competence, Inc.

<mailto:dave@corecom.com>



Security Inhibitors for EtherLECs

◆ Bandwidth & Risk

- Given, the same window of opportunity, an attacker can copy more information from a compromised system over a fast connection than a slow one.
- The attacker can also be more destructive.

◆ Ethernet Services History

- “Shared” cable modem passings



Security services sought from EtherLECs (public “MAC” level)

- ◆ Separation of customer traffic
- ◆ Protection from traffic capture, monitoring, and replay
- ◆ Bandwidth management
- ◆ Denial, disruption, or theft of access service
- ◆ Service masquerading
- ◆ Traffic misdelivery
- ◆ Monitoring, logging, auditing, reporting
- ◆ Physical security



Security services sought from EtherLECs (IP level)

Any IP security service you'd build or buy...

- ◆ Firewall
- ◆ VPN
- ◆ Authentication (e.g., RADIUS, PKI)
- ◆ Intrusion Detection
- ◆ DDOS prevention/protection
- ◆ Monitoring, logging, auditing, reporting
- ◆ Physical security



“Access Play” influences security services from EtherLECs

◆ Pure Play MAC service

- Access terminates at public ISP partner, affiliate POPs
- Access terminates at enterprise IDC’s and DC’s
- EtherLEC responsible for MAC level security services, IP is *someone else’s problem*

◆ MAC+IP service

- Access includes MAC and IP switching
- EtherLEC steps up to MAC and IP level security (like MSP)



How they do it

- ◆ Telseon
- ◆ XO Communications
- ◆ Yipes

For more information, see
EtherLECs and Security

<http://www.clec-planet.com/business/2001feb12piscitello.html>