VoIP Resilience and Security

Jim Credland

beyond communications | thus

About …

- **THUS plc**
  - Provider and user of VoIP and Soft Switch technologies
  - Developing Enterprise Security Standards
- **NISCC VoIP Working Group**
  - Security Considerations for VoIP Service Providers
- **NICC Security Group**
  - Interconnect Security Standards for Service Providers

thus

VoIP Variations

- Internet based peer-to-peer services
  - Skype
- Internet based commercial services
  - Vonage
  - SkypeOut
- Invisible carrier PSTN replacement
  - THUS's NGN
  - VoIP Peering
  - PSTN Peering
- Carrier VoIP tails
- Enterprise VoIP with PSTN interface

Converging Threats

→**Converging technologies**

→Laptop now used for e-mail, IM, telephone calls

→Same cable, same switching

→**Converging Threats**

→Voice call destinations could be secure or could be insecure

→Denial-of-Service attacks can now easily affect your telephone service

→Laptop with tcpdump can now reveal phone conversations

→Phishing attacks using VoIP!

→SPIT

thus

Goals: Set Your VoIP Security Goal

→ Set your VoIP Security Goal

- → Better Security
  - → Encryption, Strong Authentication, High Availability
- → Similar Security
- → Lower Security
- → Different Security
  - → Pick and choose from confidentiality, integrity and availability.

thus

Reducing the Risks at the Provider

- **Separation**
  - MPLS
  - Separate networks, routers.
  - Enhancing Internal Security
- **Denial-of-Service attacks**
  - Separate edge routers for private and Internet services.
- **Delivery of Secure Services to Customers**
  - Limited by available technologies

Reducing the Risks at the Customer

→ Maintain Separation

- → Switch Security
- → vLANs
- → Separate inter-site VPN for Voice?

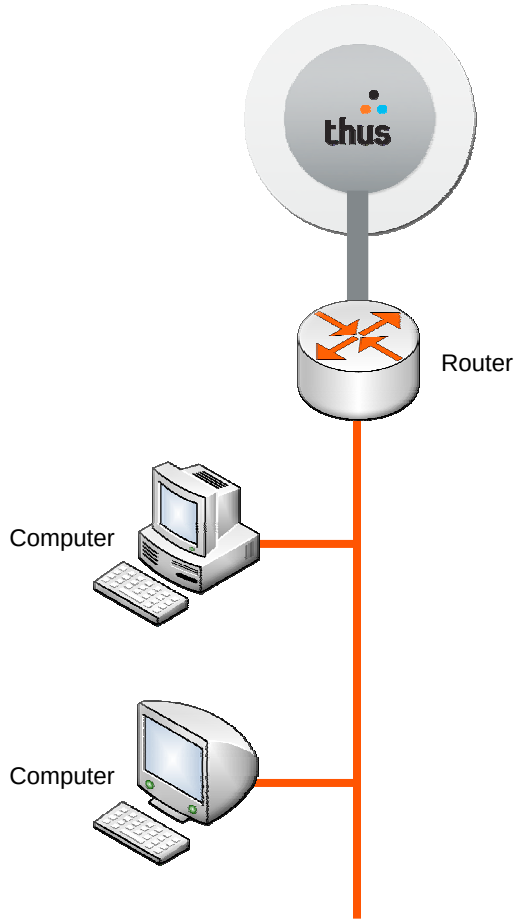
- → Separate networks, routers – not cost effective?

- → Enhancing Internal Security

→ Encryption and Authentication

- → More control over environment means better chances of success.
- → Encryption and authentication do not always deliver availability, but succeed in confidentiality and integrity.

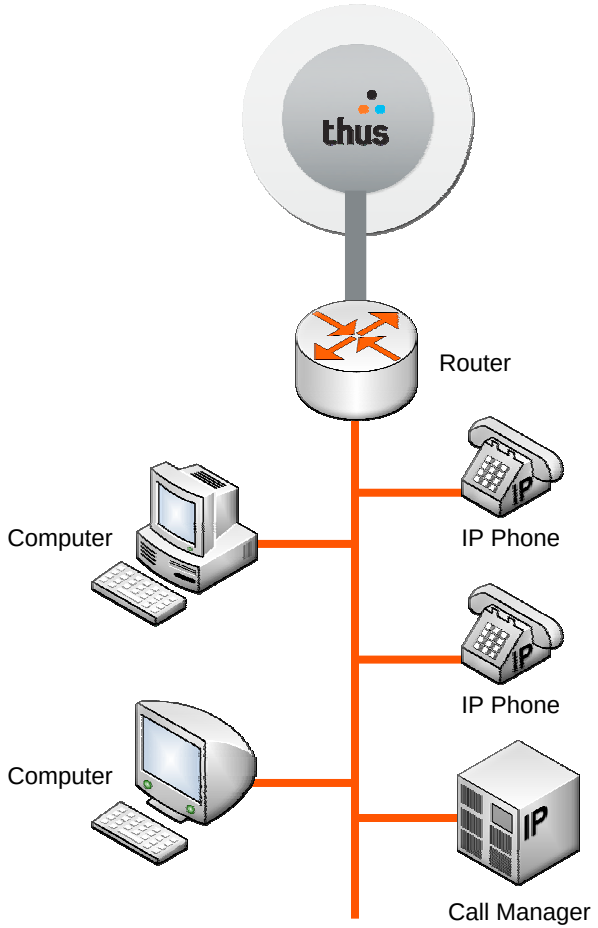
Customer: Basic Network



thus

Customer: Trivial Risky Implementation

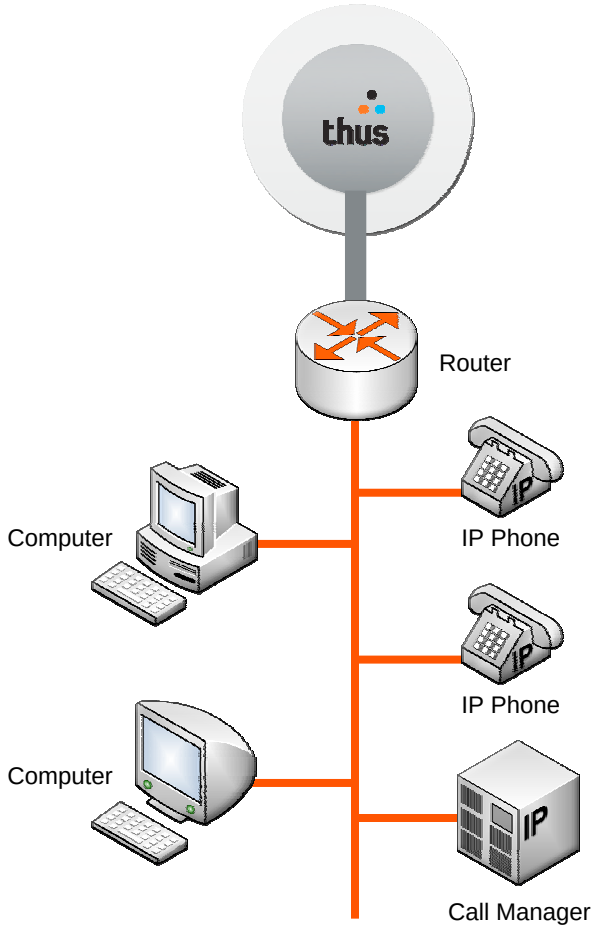
- IP Phones plug into same switches and hubs
- Risks
  - Vulnerable to virus and worm attacks
  - Eavesdropping by insides or external parties relatively trivial
  - Considerably less secure and reliable than standard analogue PBX solution
  - Hacked PC could easily make phone calls – Toll Fraud



thus

Customer: Trivial Implementation – Counter measures

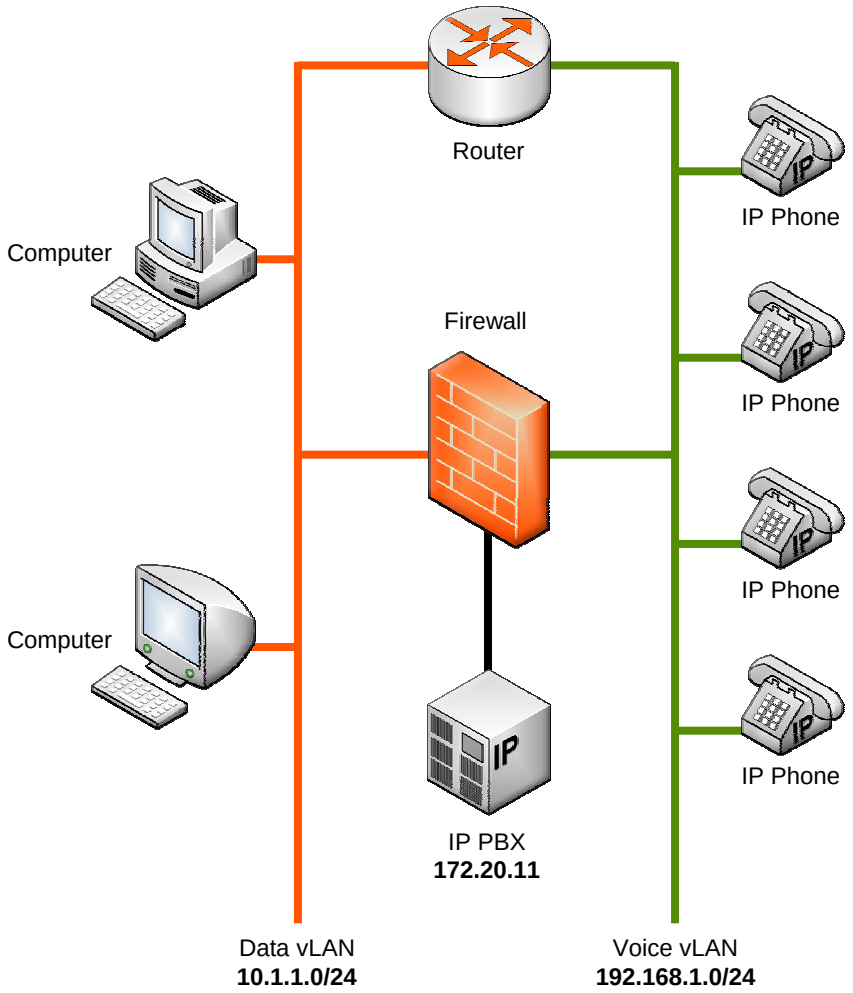
- IP Phones plug into same switches and hubs
- Countermeasures
  - Run encryption and strong authentication
  - Requires more expensive phones and more complex configuration
  - Doesn't reduce risk from denial of service type problems, phones may be disrupted by virus or other local network issues



thus

Customer: Dual LAN Solution

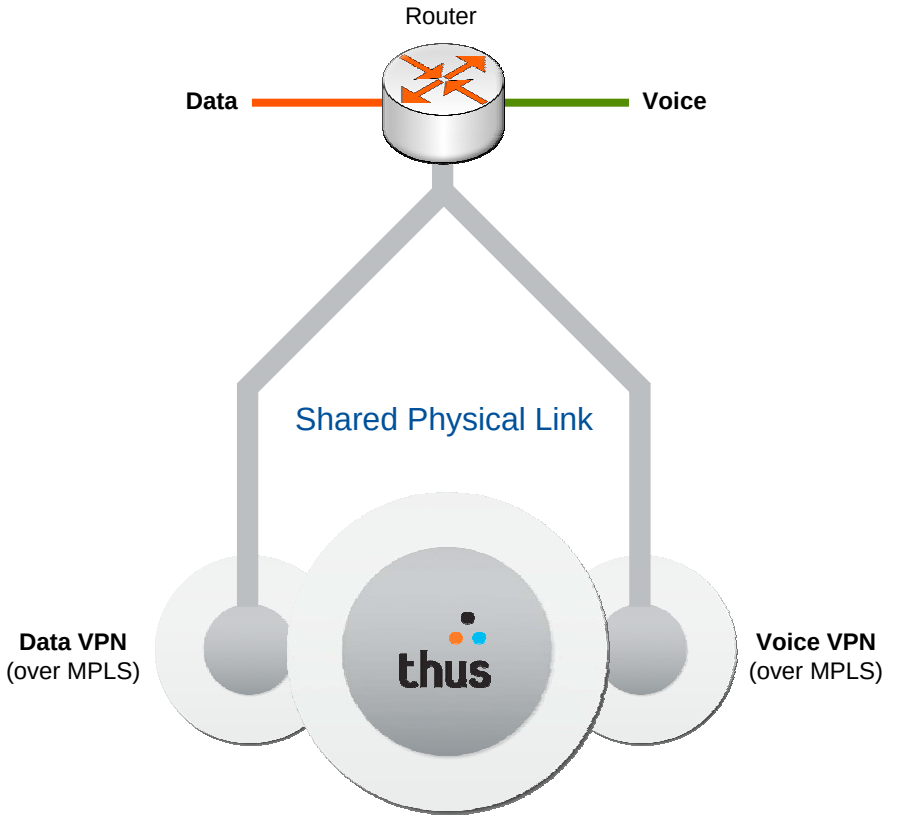
- Solves most common security issues
  - Even following Cisco SAFE recommendation there may still be denial-of-service attacks possible, but difficult.
- More complex configuration
  - Requires careful audit of switch configuration
  - Allows telephone network to achieve almost the same level of security as a standard analogue system
  - With encryption and strong authentication telephone system may even by some measure be more secure.



Customer: WAN Solutions

- Dual WAN
  - Share physical links
  - Run tagged vLANs to your Ethernet switches
  - Separating networks like this leads a simpler security configuration
  - Easier to audit - fewer potential gateways from Voice to Data LAN

Voice and Data vLAN:
Communication blocked by default



thus

Questions ... ?

jim.credland@thus.net

beyond communications | thus